

## Table of Contents

<b>Written Submission .....</b>	<b>2</b>
1. University of Fiji .....	3
2. University of South Pacific (USP).....	13
3. Fiji Law Society (FLS).....	15
4. Fiji Independent Commission against Corruption (FICAC).....	57
5. Fiji Intelligence Unit (FIU).....	60
6. Citizens Constitutional Forum (CCF).....	87
7. Ms. Salanieta Tamanikaiwaimaro.....	90
8. Datec Fiji Limited.....	101
9. Fiji Police Force .....	103
10. Office of the Director of Public Prosecutions.....	109
11. Fiji Women Crisis Centre.....	115
12. Wespac Banking Corporation.....	124
13. Fiji Revenue and Customs Services (FRCS).....	125
14. Bank of south Pacific (BSP).....	131
15. Ministry of Defence, national security and Policing.....	134
16. Mr. Alexander Horne.....	140
17. Software Factory Limited.....	145
18. Pacific Islands Forum Secretariat (PIFS).....	147
19. Online safety Commission (OSC).....	151
20. Ministry of Home Affairs and Immigration.....	153
<b>Verbatim Reports .....</b>	<b>159</b>
1. University of Fiji .....	160
2. Ministry of Communications.....	176
3. USP, FLS, FWRM .....	199
4. FICAC, UNOCHR, FIU, CCF .....	217
5. Ms. Tamanikaiwaimaro, DATEC, FPF, FHRADC .....	249
6. DPP and FWCC.....	279
7. FRCS and BSP.....	298
8. Sole limited and PIFS.....	312
9. Online safety Commission (OSC).....	330
10. Ministry of Home Affairs and Immigration.....	342

# Written Submission



**The University of Fiji**  
(An Entity of Arya Pratinidhi Sabha of Fiji)

**Submission to the Fiji Parliament Standing Committee on Foreign  
Affairs and Defence on Cybercrime.**

**Professor Shaista Shameem, Vice Chancellor**

**Professor Shawkat Ali, School of Science and Technology**

**Professor Aziz Mohammed, JDP School of Law**

**Ms Varsha Bano, JDP School of Law**

**Mr Farik Mohammed, School of Science and Technology.**

**A. Introduction.**

The University of Fiji through its Schools of Law and Science and Technology appreciates the opportunity provided by the Hon. Parliamentary Standing Committee on Foreign Affairs and Defence to make submissions on this very important Convention, namely the Convention on Cybercrime (otherwise known as the Budapest Convention).

The submissions cover both legal and Information Technology issues that the University of Fiji is able to provide to the Hon. Committee. The University will be able to answer any questions that the Hon. Members of the Committee may have in regards to the submissions.

## **B. Legal Issues**

### **(i) Harm minimized by accession.**

Fiji no longer functions in isolation. Modern technology and developments have brought the international community together. We are faced with similar cybercrime crises as experienced elsewhere. The effects of cybercrime are well known. The harm it has caused include financial losses, as well as harm to economic and social aspects has left a lasting effect. Investigating and prosecuting offenders has become a challenge particularly when the victim, offender and the providers are located in separate countries. The so-called cloud computing age has become a test.

Undoubtedly, the Convention will improve mutual cooperation across territories, aiding in investigations and prosecutions. Accession to the Convention would benefit Fiji in addressing trans-border crime. So far, this Convention is the only international treaty seeking specifically to address internet and computer crime. We know how important and effective International cooperation is, especially when dealing with trans-border cybercrime.

The Convention is a cybercrime treaty in title, but its benefits encompasses more. Its provisions deal with pure cybercrime, cyber-enabled crime and criminal evidence stored electronically. In acceding to the Convention, we will be required to incorporate the following into our domestic legislation:

- a) offences against the confidentiality, integrity and availability of computer data and systems;
- b) computer-related offences such as fraud or forgery;
- c) content-related offences such as the distribution of child pornography through computer systems; and
- d) offences related to commercial-scale infringements of copyright and theft of intellectual property.

We will also be required to regularize search and surveillance powers necessary for obtaining electronic evidence of offending, consistent with domestic and international human rights obligations. These include:

- a) measures to order the expeditious preservation of subscriber data, traffic data and content data;
- b) measures to order the production of specified computer data and subscriber information;
- c) measures to enable search and seizure of stored computer data; and
- d) measures to collect traffic data associated with specified communications in real-time, and, in relation to serious offences, measures to collect computer content data in real time.

The Convention includes provisions requiring that enforcement powers and procedures established under the Convention are to be conducted with adherence to fundamental human rights and freedoms, including freedom of expression, respect of privacy and personal data. This allows the ordinary public constitutional protection but, at the same time, does not permit offenders to take refuge in impunity.

The Convention sets out several principles and procedures related to international cooperation. These include:

- a) procedures relating to mutual assistance and the collection and sharing of electronic evidence; and
- b) the establishment of a 24-hour designated point of contact to ensure the provision of assistance between parties for the investigation of cybercrime.

Accession to the Convention would enhance cooperation with member states to address cybercrime. Fiji would need to make incremental amendments to its laws to accede to the Convention. These changes would complement and enhance Fiji's international commitment on cybercrime.

## **(ii) Other related Legal instruments relevant to the Convention on Cybercrime**

The first document is the Additional Protocol to the Convention on Cybercrime. The Protocol concerns the criminalization of acts of a racist and xenophobic nature committed through computer systems. This additional protocol was the subject of negotiations in late 2001 and early 2002. Final text of this protocol was adopted by the Council of Europe Committee of Ministers on 7 November 2002 under the title "Additional Protocol to the Convention on cybercrime.

The second document associated to the Convention on cybercrime is the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic. The Second Protocol aims to further enhance co-operation on cybercrime and the ability of criminal justice authorities to collect evidence in electronic form of a criminal offence for the purpose of specific criminal investigations or proceedings through additional tools pertaining to more efficient mutual assistance and other forms of co-operation between competent authorities; co-operation in emergencies (that is, in situations where there is a significant and imminent risk to the life or safety of any natural person); and direct co-operation between competent authorities and service providers and other entities in possession or control of pertinent information. The purpose of this Protocol, therefore, is to supplement the Convention and, as between the Parties thereto, the First Protocol.

The third notable development in this respect is the proposed United Nations Treaty on Cybercrime. After years of discussion, the UN General Assembly has voted to begin negotiating a Cybercrime Treaty that has potential to reshape policing on a global scale, with serious implications for human rights. UN Resolution 74/247 created the Ad Hoc intergovernmental committee who will draft the proposed treaty. The committee held its first negotiating session from February 28th to March 11, 2022. There seems to be support on the inclusion of so-called “pure” cybercrimes like network intrusion or interference with the operation of a computing system. Also for discussion are matters associated with broader range of ‘cyber-enabled’ crimes— such as fraud or drug trafficking that do not inherently target information and communications technologies but where Information and Communication Technology.

We submit that the Convention on Cybercrime, Additional Protocol to the Convention on Cybercrime and the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic present no adverse provisions that would undermine any current domestic legislation. The three documents if adopted will only enhance Fiji’s effort in combating Cybercrime.

### C. Science and Technology Issues

Let me begin with a quote from General Sun Tzu, from the book Sun Tzu in the Art of War – The Oldest Military Treatise in the World:

“An army that is better prepared, that is highly trained, that fights an unprepared enemy, and one that makes no mistakes – is destined to win”

Sun Tzu in the Art of War

The cyberspace, better known as the Internet, is a digital warzone, where cyberwars are fought continuously between the cybersecurity professionals and cybercriminals. As defenders, we know that the cybercriminals are from one of the several categories of unethical hackers – script kiddies, blue hat hacker, hacktivist, malicious insider/whistle blower, state/nation sponsored hacker, or black hat hacker. Each category of hacker is well trained and skilled for the specific missions they want to accomplish. Some common types of cyber-attacks include denial of service (DoS), distributed denial of service (DDoS), man-in-the-middle (MITM), phishing attack, whale-phishing attack, spear-phishing attack, ransomware, password attack, structured query language (SQL) injection attack, uniform resource locator (URL) poisoning, domain name system (DNS) spoofing, session hijacking, brute force attack, web attack, insider threat, trojan horse, drive-by attack, cross-site scripting (XSS) attack, eavesdropping attack, birthday attack, and malware attack. In a cyberwar, an attacker may only need one successful attack to win, but defenders need to be successful against all attacks to win.

“Rely not on the likelihood of the enemy not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.”

Sun Tzu in the Art of War

All apps (applications), websites, application programming interfaces (APIs), and entire information systems need to be securely developed. Secure Software Development Life Cycle (SecSDLC) model must be used for all software engineering projects. In SecSDLC, security is

integrated in each phase of the development life cycle, so that security gets built-in from the very core and is not left to be considered as an after-thought.

It is important to Identify and Fix Vulnerabilities in information systems. All information systems that render critical services is made up of components such as hardware software, networks, procedures, data, and people. Each of these components must be secured against critical, and high-level vulnerabilities.

Network defenders can use network vulnerability assessment software such as Tenable Nessus to identify critical, high-, and low-level vulnerabilities (weaknesses) in operating system, applications software, and the network protocols in use in relation to imminent threat. The resulting report can be used to provide necessary fixes in relation to the imminent threat to neutralise the resulting attack as well as associated risk. Moreover, most vulnerabilities in software and hardware can be eliminated by upgrading to latest version or applying software or firmware updates. Also, Fiji should not allow technology sellers to import obsolete and insecure software, endpoint devices, and network technologies into the Fijian market. Such technologies will only make the fight against cyberattacks more difficult.

The Internet is a powerful vehicle for many services that benefit humanity. Accessing e-government services, social networking, emailing, web browsing, web search, remote working, online studies, e-shopping, e-banking, e-bill payment, and mobile top-up are some of the most common activities that people in Fiji use the Internet for. However, the Internet is also a Pandora's box through which hackers target the confidentiality, integrity, and availability of an of data and critical services. For example, if an SQL injection attack succeeds, several things can happen, including the release of sensitive data or the modification or deletion of important data. We need to develop secure databases and data entry forms, (2) implement encryption to ensure confidentiality of Personal Identifiable Information (PII), (3) better hash algorithms to ensure integrity of data, and (4) implement robust distributed systems and backup systems to ensure 24/7/365 availability of information and critical services from our network infrastructures.

Also, a White Hat Hacker is often contracted by businesses as a penetration tester to perform further security tests by trying to actively penetrate system weaknesses. The tester than reports back to the business explaining how bad the situation is, and if anything requires fixing, the

tester guides how to fix the problem. When a vulnerability is fixed in time, the related threat is neutralized, and the related attack will not pose risk. For example, A penetration tester may send a tempting phishing email to test end-users (people) who can fall victim to such attacks. Those who click on the link, are the vulnerable people in the system who need urgent cybersecurity awareness training against phishing attacks. When people are aware about how to inspect emails for signs of phishing, can positively identify an email as phishing email, and then does not action the attacker's link in the message, the attack is neutralized. Also, to reduce the risk of insider attacks, the principle of least privilege, also called "least privilege access," is implemented so that a user only has access to what he absolutely needs to perform their responsibilities, and no more.

For secure procedures, defenders should utilize international standards such as ISO/IEC 27001 – Information Security Management, ISO/IEC 27002, ISO/IEC TS 27100 – Information technology – Cybersecurity, and ISO/IEC TS 27110 – Information technology – Cybersecurity and privacy protection. Correct application of these standards ensures that our information systems have adequate controls in place for cybersecurity.

“Being skillful in attack means that the enemy does not know what to defend and being skillful in defense means that the enemy does not know what to attack.”

Sun Tzu in the Art of War

Cybersecurity is a game of attack and defense. To defend against cyber-attacks, one needs to think like an attacker. Every attack is carefully planned and executed using the attack model - Cyber Kill Chain. In step 1, Reconnaissance phase of Cyber Kill Chain, the attacker probes for a weakness. This might include harvesting login credentials or information useful in a phishing attack. In step 2, Weaponization phase, the attacker builds a deliverable using an exploit and a backdoor. In step 3, Delivery, the attacker sends the weaponized bundle to the victim. For example, sends a malicious link in a legitimate looking email. In step 4, Exploit phase, the malicious code is activated and executed on the victim's system. In step 5, Installation phase, the malware is installed on the target asset. In step 6, Command and Control (C&C) phase, a channel gets created for the attacker to control the system remotely. In step 7, Action phase, the attacker

remotely carries out his intended goal. Just like the attackers, the defenders can also use the Cyber Kill Chain to test their system for security weakness

Moreover, cybersecurity can be strengthened by applying defense-in-depth and layered security mechanisms. Layered security is implementing multiple products to address one single aspect of security. Using seemingly redundant products strengthens the enterprise's defense against threats. For example, a gateway and a firewall both determine which data should be allowed to enter the network. There are certainly differences between the two—a gateway is hardware while a firewall is both hardware and software—but they both aim to restrict access to certain websites and applications. Once the gateway and firewall have done their jobs—an employee has been allowed to visit a particular website, for example—another security product or service will have to take over if the employee wants to enter a password to log in to that website. The next security product can be multi-factor authentication (MFA), which prevents access to a website unless multiple credentials are provided. In other words, layered security only addresses one dimension of security or one vector of attack while defense-in-depth is broader, multi-faceted, and more strategic in scope.

A layered security strategy is implemented using three different controls: administrative, physical, and technical. Administrative controls include the policies and procedures needed to restrict unauthorized access, such as role-based access control (RBAC) or employee training to protect against phishing scams. Physical controls incorporate physically securing access to the IT system, such as locking server rooms, while technical controls include the mix of products and services the organization selects to address security. Core layers to carry out a defense-in-depth strategy should include (1) strong, complex passwords, (2) antivirus software, (3) secure gateway, (4) firewall, (5) patch management, (6) backup and recovery, and (7) the principle of least privilege, or giving a user the minimum access level or permissions needed to do his or her job. Then as companies grow and the number of devices, applications, and services used across the organization increases, these serve as important security layers in a defense-in-depth strategy such as applying (1) two-factor authentication (2FA) or multi-factor authentication (MFA), (2) intrusion detection and prevention systems, (3) endpoint detection and response (EDR), (4) network segmentation, (5) encryption, and (6) data loss prevention (DLP).

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every battle gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

Sun Tzu in the Art of War

With the right cybersecurity awareness, training, skills, and experiences Fijians can win against sophisticated cyber-attacks. However, as new technologies emerge, new threats and vulnerabilities will emerge, and defenders will need to learn new ways to defend as adversaries learn new ways to attack.

Thus, to conclude, membership of Convention on Cybercrime (Budapest Convention) will allow Fiji to gain from experiences of international partners in the fortification and development of secure digital infrastructures in the battle against cyber-attacks.

September 26, 2022

Hon. Alexander O'Connor

**CHAIRPERSON**

**Standing Committee on Foreign Affairs and Defence**

P.O. BOX 2352, GOVERNMENT BUILDING, SUVA

PHONE 3225 600, FAX: 330 5325

PARLIAMENT COMPLEX,

Dear Hon. O'Connor,

**Subject: Budapest Convention on Cybercrime**

Thank you for inviting The University of the South Pacific (USP) to submit comments on the Budapest Convention on Cybercrime (Budapest Convention).

The Budapest Convention provides the necessary framework for international cooperation in fighting cybercrime. USP therefore supports Fiji in joining the Budapest Convention if Fiji wishes to do so.

**Human Resources Development**

USP offers a number of courses in its undergraduate and postgraduate programs in the areas of Cybercrime and Cybersecurity in general. Through its various courses in the different programs, USP empowers the future workforce with the right knowledge and resources and helps create a well-equipped and trained society to fight cybercrime.

**ICT Enterprise Practitioner**

In terms of ICT services capability, USP stands ready to continue support the Fiji Government and indeed, the regional governments, in their adoption of the Budapest Convention against cybercrime.

Further to this, USP's internet presence in the global research and education network is brokered through the Australian Academic and Research Network (AARNET) which essentially compels USP to comply with the Budapest Convention, given that Australia is already a signatory.



The University of the South Pacific  
Private Mail Bag, Laucala Campus  
Suva, Fiji

Ph: (679) 323 2053  
Email: [jito.vanualailai@usp.ac.fj](mailto:jito.vanualailai@usp.ac.fj)  
[www.usp.ac.fj/education](http://www.usp.ac.fj/education)

Yours sincerely,



+++++

Professor Jito Vanualailai,

Deputy Vice-Chancellor (Education),

The University of the South Pacific, Suva, FIJI

Email: [jito.vanualailai@usp.ac.fj](mailto:jito.vanualailai@usp.ac.fj)

Phone: +679 323 2053

URL: [www.usp.ac.fj/office-of-the-deputy-vice-chancellor-education/](http://www.usp.ac.fj/office-of-the-deputy-vice-chancellor-education/)

+++++

*Ps.110:5, 89:52*



LEX EST TUTISSIMA CASSIS

## FIJI LAW SOCIETY

PRIVATE MAIL BAG, GOVERNMENT BUILDINGS, SUVA

Phone Contact: (679) 3319390/7736146 Email: [flssecfiji@gmail.com](mailto:flssecfiji@gmail.com)

---

### FLS submissions on the Convention on Cybercrime (otherwise known as the Budapest Convention).

Mr Chairperson, Honourable Mr Alexander O'Connor of the Standing Committee on Foreign Affairs and Defence and other members, it is a privilege to submit on the Convention on Cybercrime on behalf of the Fiji Law Society its President, Mr William Wylie Clarke, Council and members to you this morning. With me is Ms Lilian Mausio of FNU who is here in her capacity as an individual, Ms Lavenia Bogitini of SLS Legal & Mr Robakeibau Nayacalevu of FLS Secretariat.

While you may hear from many groups on its submissions on this Convention ultimately it is this Committee and Parliament as the Arm of Legislature who will have the final say. Our role is to simply assist on whether this proposed Convention would benefit the country. While 67 countries are parties to this Convention, Fiji is part of the 15 countries including NZ and Vanuatu who have been invited to accede this law. However, Fiji would need to implement the provisions of this Convention before the rest of the parties agree to it being part of this Convention.

### Comments/Notes

Article	Comments
Article 1 Chapter I – Use of terms Article 1 – Definitions For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b	<p>The definitions of <i>computer system</i>, <i>computer data</i>, <i>service provider</i> &amp; <i>traffic data</i> are similar to the definitions in the Cybercrimes Act 2021 ("CCA") which commenced on 12<sup>th</sup> February 2021. The CCA has repealed Part 17 of the Crimes Act Division 6 Computer offences sections 336 – 346 and inserted consequential amendments.</p> <p>Although most of these definitions are already part of the Cybercrimes Act 2021 there is need to amend this Act to include more definitions that will help Fiji meet the provisions of the Convention. Speaker 2 will deal an example where there is a need to define "content data". Although the Convention deals with Cybercrime there is no</p>

<p>"computer data" means any representation of facts, information or concepts in a form</p>	
---	--

<p>suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.</p> <p>d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.</p>	<p>definition of cybercrime in the Article. Since Fiji has passed the Cybercrimes Act 2021, the definition of cybercrime can be included to provide citizens with more clarity and guidance. This were also submitted by Fiji Law Society in it's earlier submissions.</p> <p>Furthermore, we rely on the earlier submissions by Fiji Law Society on the Cyber Crime Bill on the definition of authorised person to include any person appointed by Officer of Director of Public Prosecutions as opposed to FICAC.</p> <p>Don't Accede as there are already part of the Cyber Crimes Act 2021 however there is some more definitions that are missed out which will be discussed by Speaker 2.</p> <p>However, there are some definitions which were excluded in the CCA and this</p> <p>Convention: "content data", "cybercrime" we can follow the provisions from Philippines.</p>
---	---

<p>Article 3 – Illegal interception</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p>Article 3 – is similar to the provisions of Section 6 of the Cyber Crimes Act 2021 which provides for the offence and its penalties.</p> <p>Do not Accede</p>
<p>Article 4 – Data interference</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.</p> <p>2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.</p>	<p>Article 4 is already similar to Sections 6, 7 and 8 of the Cyber Crimes Act 2021 which provides for unauthorised access, unauthorised interception, acts and unlawful supply or possession of computer data or data.</p> <p>Do not Accede</p>
<p>Article 5</p> <p>Article 5 – System interference</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.</p>	<p>Article 5 is already similar to the provisions of computer systems in Sections 5, 6, 7 and 8 of the Cyber Crimes Act 2021 as to unauthorised access, unauthorised interception, acts and unlawful supply or possession.</p> <p>Do not Accede</p> <p>While we welcomed laws that will help deal with cybercrime, we cannot have duplicity of laws. We have already implemented the Cyber Crimes Act 2021, is absolutely necessary to have another legislation on a similar subject matter?</p>

<p>Article 6</p> <p>Article 6 – Misuse of devices</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: the production, sale, procurement for use, import, distribution or otherwise making available of:</p> <p>i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;</p> <p>ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,</p> <p>with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and</p> <p>b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.</p> <p>2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorized testing or protection of a computer system.</p> <p>3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.</p>	<p>Article 6 is already dealt with in Section 8 of the Cyber Crimes Act 2021 but to make it more specific a definition of device needs to be provided so there is no ambiguity. This can be included in the Cyber Crimes Act 2021.</p> <p>Do not Accede</p>
--	---

<p>Article 7</p> <p><i>Title 2 – Computer-related offences</i></p> <p>Article 7 – Computer-related forgery</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.</p>	<p>Article 7 is already included in Section 9 of the Cyber Crimes Act 2021 but certain measures need to be made on establishing intent for corporate bodies. This can be dealt with through an amendment of the Act.</p> <p>Do not Accede</p>
<p>Article 8</p> <p>Article 8 – Computer-related fraud</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:</p> <p>a any input, alteration, deletion or suppression of computer data,</p> <p>b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.</p>	<p>Article 8 is already set out in Section 10 of the Cyber Crimes Act 2021 but certain measures need to be made on establishing intent for corporate bodies. This can be dealt with through an amendment of the Act.</p> <p>Do not Accede</p>

<p>Article 9</p> <p><i>Title 3 – Content-related offences</i></p> <p>Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system;</p> <p>b offering or making available child pornography through a computer system;</p> <p>c distributing or transmitting child pornography through a computer system;</p> <p>d procuring child pornography through a computer system for oneself or for another person;</p> <p>e possessing child pornography in a computer system or on a computer-data storage medium.</p> <p>2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:</p> <p>a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct.</p> <p>3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.</p> <p>4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, subparagraphs d and e, and 2, subparagraphs b and c.</p>	<p>The protection of our children particularly towards offences relating to child pornography needs to be properly drafted. It is our submission that this needs to be included in the Crimes Act 2009, the existing Cybercrimes Act 2021 or the Juveniles Act.</p> <p>This Article is already dealt with in Section 36 of the Cybercrimes Act 2021 which dealt with consequential amendments and which made amendments to Section 62A of the Juveniles Act 1973 by deleting the previous definition of pornographic activity and substituting the definition of pornographic activity.</p> <p>However, the above amendment does not deal with all the elements covered in Article 9. It is our proposal that this be amended and included in the Crimes Act 2009 to be dealt with by the office of the Director of Public Prosecutions.</p> <p>They have prosecuted such offences using the provisions of Juveniles Act namely, Pornographic activities involving juveniles: Contrary to Section 62A (1)(b) of the Juveniles (Amendment) Act 1997 in State v Koronibau [2019] FJHC 1175; HAC173.2015 (30 September 2019) so including it in the Crimes Act 2009 will assist the office in charging under these provisions.</p> <p>Accede but to include in the Crimes Act 2009</p>
--	---

<p>Article 10</p> <p><i>Title 4 – Offences related to infringements of copyright and related rights</i></p> <p>Article 10 – Offences related to infringements of copyright and related rights</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed willfully, on a commercial scale and by means of a computer system.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations (Rome Convention), the Agreement on Trade-Related Aspects of</p>	<p>Infringement of copyright and related rights can be dealt with under the provisions of the Copyright Act and other Conventions that Fiji is a party to.</p> <p>Do Not Accede</p>
---	---

<p>Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed willfully, on a commercial scale and by means of a computer system.</p> <p>3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.</p>	
<p>Article 11</p> <p><i>Title 5 – Ancillary liability and sanctions</i></p> <p>Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c of this Convention.</p> <p>3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.</p>	<p>It is not compulsory to include Article 11 as this can be included in the Cyber Crimes Act 2021.</p> <p>Do Not Accede</p>

<p>Article 12</p> <p>Article 12 – Corporate liability</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person.</p> <p>2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.</p> <p>3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.</p> <p>4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.</p>	<p>Article 7 and 8 deal with offences that may include corporate bodies which is already covered in Section 9 and 10 of the Cyber Crimes Act 2021. The element of intent needs to be clearly defined in Section 9 of the Act. There needs to be a balancing of Corporate liability in this section and the Companies Act 2015 and its regulations.</p> <p>Do Not Accede</p>
--	---

<p>Article 13</p> <p>Article 13 – Sanctions and measures</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.</p> <p>2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-</p>	<p>This is already provided for in Section 5-12 of the Cybercrimes Act 2021 which has created sanctions and measures through offences.</p>
--	--

<p>criminal sanctions or measures, including monetary sanctions.</p>	
<p>Article 14 Section 2 – Procedural law  <i>Title 1 – Common provisions</i>  Article 14 – Scope of procedural provisions  1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.  2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention;  b other criminal offences committed by means of a computer system; and  c the collection of evidence in electronic form of a criminal offence.  3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21.  Each Party shall consider</p>	<p>This is already provided for in Section 15 of the Cybercrimes Act 2021.</p>

<p>restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21</p>	
<p>Article 15 Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human</p>	<p>Article 15 requires parties to uphold the protection of human rights and liberties, including rights arising out of obligations undertaken under various human rights treaties. The treaties mentioned in Article 15 include the European Convention for the Protection of Human Rights and Fundamental Freedoms ('the European Convention') and the International Covenant on Civil and Political Rights ('ICCPR') which, although universal, do not reflect this new technological era, nor the novel problems arising out of it – one of the main ones being issues of privacy of individuals.</p> <p>For instance, the European Convention only makes reference in passing to the 'right to the respect for one's private and family life, home and correspondence, and that no public authority shall interfere with this right', while the ICCPR provides for protections against arbitrary or unlawful interference with one's privacy. Since these treaties came into force, new technologies</p>

<p>Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.</p> <p>2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or</p>	<p>have emerged, therefore falling outside the scope of the aforementioned treaties and their privacy protections. Key notions such as 'privacy', 'correspondence' and what constitutes 'interference' in the modern</p>
<p>power concerned, <i>inter alia</i>, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.</p> <p>3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.</p>	<p>context are therefore ambiguous, in the light of these technological advancements. Local legislation will need to properly define the meanings and ambit of these terms.</p> <p>Furthermore, Article 15 does not clarify what procedures are needed to safeguard human rights, and parties are left to balance such procedures against potential human rights issues, specifically privacy. This is worrying, as it creates a lacuna, for instance, in a country which may have a poor record of safeguarding privacy protection. In upholding the spirit of this Convention, any local legislation, whether already in force or yet to be enacted, must take up the mantle of explaining the scope of and providing for procedural safeguards that protect the public from potentially intrusive enforcement mechanisms. It can do this by clarifying what constitutes excessive enforcement surveillance and defining important terms such as 'privacy' and the aforementioned terms.</p> <p>That being said, we are aided by case-law from other jurisdictions which seek to address the concerns above. An example is when the European Court of Human Rights, in the case of <i>Copland v the United Kingdom</i> [2007] ECHR 253, held that telephone data, emails, Internet use and data stored on computer servers all fall within privacy protection rights<sup>1</sup> under the treaties mentioned in Article 15.</p>

<sup>1</sup> Specifically, they fall within the scope of protection of Article 8(1) of the European Convention.

<p>Articles 16 &amp; 17</p> <p><i>Title 2 – Expedited preservation of stored computer data</i></p> <p>Article 16 – Expedited preservation of stored computer data</p> <p><sup>1</sup> Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.</p> <p><sup>2</sup> Where a Party gives effect to paragraph 1 above by means of an order to a person to</p>	<p>Articles 16 &amp; 17 are already provided in Sections 18 and 19 of the Cybercrimes Act 2021 however these provisions need to have strict guidelines for the instances they are issued without the sanction of the Court. The Committee needs to balance the need to apply this provision with that of the individual rights and the need for a balanced investigation.</p> <p>Articles 16 and 17 require parties to adopt legislation instructing people and businesses to preserve data when ordered to do so by authorised persons.</p> <p>Article 16(2) requires a person to preserve such data transmission for an ‘adequate period of time’, while Article 17 goes further by requiring data to be preserved regardless of the involvement of multiple service providers.</p>
--	---

<p>preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.</p> <p><sup>3</sup> Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.</p> <p><sup>4</sup> The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p> <p>Article 17 – Expedited preservation and partial disclosure of traffic data</p> <p><sup>1</sup> Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:</p> <ul style="list-style-type: none"> <li>a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and</li> <li>b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to</li> </ul>	<p>Again, this creates a tenuous line between effective enforcement procedures and privacy of individuals. Without proper procedural safeguards in place, the scope for this Article could be used by authorities to enforce surveillance or policies unrelated to actual cyber-related crimes. Does this then open up the possibility of political surveillance or other activities unrelated to cybercrimes?</p> <p>Any local legislation must therefore provide for clear definitions and scopes to avoid the above concern.</p>
--	---

<p>identify the service providers and the path through which the communication was transmitted.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. Article 17 – Expedited preservation and partial disclosure of traffic data</p>	
---	--

<p>1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	
<p>Article 18 <i>Title 3 – Production order</i> Article 18 – Production order</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p> <p>3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or</p>	<p>Article 18 is already set out in Section 21 of the Cybercrimes Act 2021 although this provision should be amended and be confined to the order of the Court and not extended at the discretion of the police or authorised office. This sort of provision can lead to an abuse of power and can cause irreparable harm to reputation and business.</p>

<p>content data and by which can be established:</p> <p>a the type of communication service used, the technical provisions taken thereto and the period of service;</p> <p>b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.</p>	
---	--

<p>Article 19</p> <p><i>Title 4 – Search and seizure of stored computer data</i></p> <p>Article 19 – Search and seizure of stored computer data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:</p> <p>a a computer system or part of it and computer data stored therein; and</p> <p>b a computer-data storage medium in which computer data may be stored in its territory.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or</p>	<p>Article 19 is already set out in Section 21 of the Cybercrimes Act 2021. We would propose that this Section of the Cybercrimes Act 2021 be deleted and instead that it be confined to a court order.</p> <p>Article 19 allows for the search and seizure of stored computer data. It specifies how authorised persons may monitor data transmissions, but opens up the possibility of unnecessary intrusion into individual lives and matters unrelated to any potential crime because the scope of the Article is wide and encompassing. The Convention needs to add an addendum or make a footnote setting a definitive standards or guidelines so as to prevent said unnecessary intrusion.</p>
--	---

<p>similarly secure computer data accessed according to</p>	
---	--

<p>paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system.</p> <p>4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.</p> <p>5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	
--	--

<p>Article 20 &amp; 21</p> <p><i>Title 5 – Real-time collection of computer data</i></p> <p>Article 20 – Real-time collection of traffic data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:</p> <p>a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability:</p> <p>i to collect or record through the application of technical means on the territory of that Party; or</p> <p>ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.</p>	<p>Article 20 is already provided in Section 22 of the Cybercrimes Act 2021. Article 21 is already set out in Section 23 of the Cybercrimes Act 2021.</p> <p>Article 20 allows authorised persons to conduct real-time collection of traffic data, while Article 21 provides for interception of content data. The Convention does not define what ‘content data’ means, but it is implied that it is a subcategory of traffic data. Our local legislation needs to provide a definition of ‘content data’ as opposed to ‘traffic data’ so that authorised persons / law enforcement may then be able to either enact or adhere to specific guidelines when intercepting or collecting data transmissions. Again, this ties in with the privacy protection issue.</p> <p>The power given to law enforcement regarding surveillance in these two Articles is substantial, and thus should be complemented with specific guidelines that would curtail any possibility of unnecessary intrusion or privacy rights violations.</p>
--	---

<p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. Article 21 – Interception of content data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability:</p> <p>i to collect or record through the application of technical means on the territory of that Party, or</p> <p>ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.</p> <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other</p>	
---	--

measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

<p>Article 22 Section 3 – Jurisdiction Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or</p>	<p>Article 22 is already set out in Section 3(1) of the Cybercrimes Act 2021</p>
<p>Article 23 Chapter III – International co-operation Section 1 – General principles <i>Title 1 – General principles relating to international cooperation</i> Article 23 – General principles relating to international co-operation The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.</p>	<p>Article 23 is already set out in Section 24 of the Cybercrimes Act 2021</p>
<p>Article 24 <i>Title 2 – Principles relating to extradition</i> Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.</p>	<p>Article 24 is already set out in Section 25 of the Cybercrimes Act 2021</p>

<p>2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.</p> <p>3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.</p> <p>4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.</p> <p>5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.</p> <p>7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.</p>	
--	--

<p>Article 26</p> <p>Article 26 – Spontaneous information</p> <p>1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.</p> <p>2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.</p>	<p>This Article is already in Section 26 of the Cybercrimes Act 2021</p>
---	--

<p>Article 27</p> <p><i>Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements</i> Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements</p> <p>1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.</p>	<p>Article 27 allows a party to refuse extradition under certain circumstances, such as crimes constituting political offenses or those that may prejudice a nation's interests. The provision, however, does not clarify what types of offences qualify as "political" in nature or which they will consider prejudicial. This provision may become ineffective simply due to the different interpretations of what constitutes a political offense. The Convention needs to provide more detailed guidance as to what types of political offences or prejudices will legitimately justify a refusal to cooperate and who will render that decision. The Convention should also either provide additional guidance to signatories or set the standards itself to ensure timely and efficient criminal investigations through international cooperation.</p>
--	--

<p>3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.</p> <p>4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p> <p>5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. Before refusing or postponing assistance, the requested Party shall, where appropriate after</p>	
--	--

<p>having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.</p> <p>7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.</p> <p>8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.</p> <p>9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.</p> <p>b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).</p> <p>c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.</p>	
---	--

<p>d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.</p>	
<p>Article 28 Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless, be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.</p>	<p>Already set out in Section 27 of the Cybercrimes Act 2021</p>

<p>Section 2 – Specific provisions</p> <p><i>Title 1 – Mutual assistance regarding provisional measures</i></p> <p>Article 29 – Expedited preservation of stored computer data</p> <p>1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.</p> <p>2 A request for preservation made under paragraph 1 shall specify:</p> <p>a the authority seeking the preservation;</p> <p>b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;</p> <p>c the stored computer data to be preserved and its relationship to the offence;</p> <p>d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and</p> <p>f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.</p> <p>3 Upon receiving the request from another Party, the requested Party shall take all appropriate</p>	<p>Article 29 is already set out in Section 28 of the Cybercrimes Act 2021</p> <p>Article 29 does not require “dual criminality” as a condition for mutual assistance for the preservation of data. This creates challenges in the context of cybercrime where one jurisdiction may not recognise the relevant conduct as an offence at all. This raises a few concerns in terms of the preservation of data. Firstly, does this imply that one country has the right to interfere with the privacy of another country’s citizens? Does this suggest that one country may impose “onerous requirements” to investigate crimes of the citizens of another country?</p>
--	---

<p>measures to preserve expeditiously the specified data in accordance with its domestic law.</p> <p>For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.</p> <p>4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.</p> <p>5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p> <p>6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a</p>	
---	--

<p>period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.</p>	
--	--

<p>Article 30</p> <p>Article 30 – Expedited disclosure of preserved traffic data</p> <p>1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.</p> <p>2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p>	<p>This article is already set out in Section 29 of the Cybercrimes Act 2021</p>
---	--

<p>Article 31</p> <p><i>Title 2 – Mutual assistance regarding investigative powers</i> Article 31 – Mutual assistance regarding accessing of stored computer data</p> <p>1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.</p> <p>2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.</p>	<p>This set out in Article 30 of the Cybercrimes Act 2021.</p> <p>Article 31 relates to mutual assistance regarding the accessing of stored computer data, makes no provision in respect of specific grounds of refusal. This Article is one of the more intrusive requests of the convention, however it is deferred to existing arrangements and/or domestic laws. The convention provides no model procedures or standards in which this can be adapted by a signatory country whilst being consistent with <i>Convention for the Protection of Human Rights and Fundamental Freedoms</i>.</p>
--	---

<p>3 The request shall be responded to on an expedited basis where:</p> <p>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or</p> <p>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.</p>	
<p>Article 32</p> <p>Article 32 – Trans-border access to stored computer data with consent or where publicly available</p> <p>A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or</p> <p>b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.</p>	<p>Already set out in Section 31 of the Cybercrimes Act 2021</p>

<p>Article 33 Article 33 – Mutual assistance regarding the real-time collection of traffic data</p> <p>1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.</p> <p>2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.</p>	<p>This set out in section 32 of the Cybercrimes Act 2021</p> <p>Article 33 which relates to mutual assistance in the real-time collection of traffic data, is specifically stated to be governed by the conditions and procedures provided for under domestic laws. The preservation of data and traffic logs are only useful in the investigation of a hacker where real time evidence can be collected and communications potentially intercepted. However, real time evidence collection and interception of communications require certain procedures for a warrant under section 22 of the Cybercrime Act 2021, this may render Article 33 ineffective in practice.</p>
<p>Article 34 Article 34 – Mutual assistance regarding the interception of content data</p> <p>The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.</p>	<p>Article 34 is set out in section 33 of the Cybercrimes Act 2021</p>

<p>Article 35  <i>Title 3 – 24/7 Network</i>  Article 35 – 24/7 Network  1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects.</p> <p>2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.</p> <p>3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.</p>	<p>Article 35 is set out in Section 34 of the Cybercrimes Act 2021</p>
--	--

<p>Article 36</p> <p>Chapter IV – Final provisions</p> <p>Article 36 – Signature and entry into force 1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.</p> <p>2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.</p> <p>3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2. 4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.</p>	<p>Chapter IV (Articles 36-48) deals with the final provisions of the convention. There is an obvious failure to include any follow-up measures to ensure that ratification is followed by compliance.</p> <p>Accede this is yet to be complied with in this Convention.</p>
--	--

<p>Article 37</p> <p>Article 37 – Accession to the Convention</p> <p>1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.</p> <p>2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.</p>	<p>Accede</p>
<p>Article 38</p> <p>Territorial application</p> <p>The Convention provides that any State may specify the territory or territories to which the Convention applies, at the time of signature or depositing its instrument of ratification, acceptance, approval or accession.</p>	<p>Accede</p>

<p>Article 38 of the Convention also allows a State to extend the application of the Convention on a later date to any other territory by declaration addressed to the Secretary General, which will come into force on the first day of the month following the expiration of a period of three months after the Secretary General has received the declaration.</p> <p>Furthermore, a declaration made can be withdrawn by notification to the Secretary General, and such withdrawal will come into force on the first day of the month following the expiration of a period of three months after the Secretary General has received the notification</p>	
<p>Article 39</p> <p>Effects of the Convention The Convention provides the purpose of the Convention which is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the European Convention on Extradition, opened for signature in Paris on 13 December 1959 (ETS No. 24), the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No.30); and the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg on 17 March 1978 (ETS No. 99).</p> <p>Where an agreement or treaty has already concluded or relations established, Parties are also entitled to apply the agreement or treaty or regulate such relations in a manner that is not inconsistent with the Convention</p>	<p>Accede</p> <p>In determining the Convention's relationship to other international agreements, Parties may look for additional guidance to relevant provisions on Agreements or Law of Treaties</p> <p>May include savings clause for unaffected other rights, restrictions, obligations, and responsibilities that may exist but that are not dealt with by the Convention. Agree.</p> <p>In determining the Convention's relationship to other international agreements, Parties may look for additional guidance to relevant provisions on Agreements or Law of Treaties May include savings clause for unaffected other rights, restrictions, obligations, and responsibilities that may exist but that are not dealt with by the Convention.</p>

<p>Article 40</p> <p>Declarations The Convention allows any State, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession to declare that it avails itself of the possibility of requiring additional elements as provided for Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27 paragraph 9.e, by written notification to the Secretary General.</p>	<p>Accede</p> <p>Declarations are considered acceptable interpretations of the Convention provisions and should be distinguished from reservations, which permit a Party to exclude or to modify the legal effect of certain obligations set forth in the Convention</p>
<p>Article 41</p> <p>Federal clause The Convention allows a federal State to reserve the right to assume obligations under Chapter II of the Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to cooperate under Chapter III.</p> <p>Article 41 of the Convention also provides that such reservation must not exclude or substantially diminish the State to provide for measures set out in Chapter II and must provide for a broad and effective law enforcement capability in relation to those measures.</p>	<p>Accede</p> <p>The approach to federalism does provides for broad coverage of illegal conduct encompasses by this Convention under Federal Criminal Law.</p> <p>The scope of application of federal clause has been restricted to the provisions of Chapter II. Federal States marking use of this provision would still under the obligation to co-operate with the other Parties under Chapter III</p>

<p>Where the application of the provisions of the Convention comes under the jurisdiction of constituent States or other similar territorial entities that are not obliged under their constitutional systems to take legislative measures, the federal governments must inform and encourage the competent authorities of such States to take appropriate action to give effect.</p>	
---	--

<p>Article 42</p> <p>Reservations</p> <p>The Convention allows any State, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by written notification to the Secretary General, to declare that it avails itself of the reservations provided for in Article 4 paragraph 2, Article 6 paragraph 3, Article 9 paragraph 4, Article 10 paragraph 3, Article 11 paragraph 3, Article 14 paragraph 3, Article 22 paragraph 2, Article 29 paragraph 4, and Article 41 paragraph 1, only.</p>	<p>Accede</p> <p>This recognises that some Parties certain reservations are essential to avoid conflict with their constitutional and legal principles, provisions and or to withdraw which no longer proof necessary</p>
<p>Article 43</p> <p>Status and withdrawal of reservations</p> <p>The Convention allows a State Party that has made a reservation to withdraw such reservation either as a whole or partially by notifying the Secretary General, which would then take effect on the date of receipt of the notification by the Secretary General or on a later date if specified on the notification.</p> <p>Article 43 of the Convention also allows the Secretary General to periodically enquire with Parties who have</p>	<p>Accede</p> <p>This gives an opportunity to Parties to indicate whether they still maintain their reservations in respect to certain</p>
<p>adopt the amendment, the text of which will then be forwarded to Parties for acceptance.</p> <p>Any adopted amendment comes into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance of the amendment.</p>	

<p>Article 45</p> <p>Settlement of disputes The Convention provides that CDPC must be kept informed regarding the interpretation and application of the Convention. Where there is a dispute between States Parties on the interpretation or application of the Convention, States Parties must seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC whose decision will be binding</p>	<p>Accede</p> <p>Provides way forward for settlement of disputes concerning interpretation or the application of the Convention.</p> <p>Procedures may outline for settlement disputes and any procedure for solving disputes resolution should be agreed upon by the parties concerned. Where will be the dispute be heard and who presides (CDPC, Tribunal or International Court)</p>
<p>Article 46</p> <p>Consultations of the Parties The Convention requires Parties to undertake periodic consultations with a view to facilitate the effective use and implementation of the Convention, exchange of information on significant legal policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form, and consideration of possible supplementation or amendment of the Convention.</p> <p>Under Article 46 of the Convention, the CDPC must be kept informed of the result of these consultations and must assist State Parties in their efforts to supplement or amend the Convention, with expenses to be borne by Parties unless assumed by the Council of Europe. The Secretariat of the Council of Europe must also assist Parties in carrying out their functions under this article.</p>	<p>Accede</p> <p>Provides for review of the Convention operations. A time frame may be included for review say for example annually or every 3 years. Agree.</p> <p>Provides for review of the Convention operations. A time frame may be included for review say for example annually or every 3 years.</p>

<p>Article 47</p> <p>Denunciation</p> <p>The Convention allows a State Party to denounce the Convention by notification addressed to the Secretary General, which would then become effective on the first day of the month following expiration of a period of three months after the date of receipt of the notification by the Secretary General.</p> <p>The Convention allows a State Party to denounce the Convention by notification addressed to the Secretary General, which would then become effective on the first day of the month following expiration of a period of three months after the date of receipt of the notification by the Secretary General.</p>	<p>Accede</p>
<p>Article 48</p> <p>Notification</p> <p>The Convention requires the Secretary General to notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of the Convention as well as any State which has acceded to, or has been invited to accede to, the Convention of any signature, deposit of any instrument of ratification, acceptance, approval or accession, date of entry into force, any declaration or reservation made and any other act, notification or communication relating to the Convention.</p>	<p>Accede</p>

GENERAL COMMENTS	<p>This Convention is undoubtedly needed, given the technological era we live in, and the transnational nature of crimes arising therefrom. However, there is a fine line between effective law enforcement procedures and certain civil liberties and rights. The current legislation must be strengthened by providing more definitive guidelines on the scope of law enforcement powers, especially with regards to “surveillance and data interception”. This Convention is undoubtedly needed, given the technological era we live in, and the transnational nature of crimes arising therefrom. However, there is a fine line between effective law enforcement procedures and certain civil liberties and rights. The current legislation must be strengthened by providing more definitive guidelines on the scope of law enforcement powers, especially with regards to surveillance and data interception.</p> <p>There is a need to be particularly cautious in adopting procedures that impact on civil liberties. However, it is of equal importance that we make Fiji a harder target for technological enabled crime. The current legislation must be strengthened and reviewed periodically. There must be a joint effort to identify trends and criminal methodologies so we are better prepared to combat future and present cybercrime.</p>
------------------	--

**SUBMISSION BY THE FIJI INDEPENDENT COMMISSION AGAINST CORRUPTION TO THE  
PARLIAMENTARY COMMITTEE ON FOREIGN AFFAIRS ON ACCESSION OF THE CONVENTION  
ON CYBER CRIME**

**Introduction**

We thank the Committee for inviting the Commission (FICAC) to make submissions. This is important at this juncture as this Committee endeavors to provide the necessary recommendations to Parliament of Fiji on the importance of joining the Budapest Cyber-crime Convention (hereinafter referred to as Convention) as state party.

Over the years, Information Technology had changed the human life drastically and will surely continue to impact all of us in the future as well. It has more often made the life easier in many aspects. It revolutionized the human interactions and methods of communication. Human interactions have become more complex, sophisticated and also overcome the distance and time barriers that were in place few decades ago.

With such technological advancement in the cyber space, the conventional criminals and fraudsters too have evolved and become cyber-complicit. Cyber universe has become an opportune conduit to advance the fraudulent and criminal activities on a different and larger scale. Many individuals and Governments fell victim to cybercrimes losing millions of dollars. There was and is a dire need to tackle the ever-increasing criminal activities via internet and computer networks.

Cybercrime has no border. No distance or geographical barriers could prevent or slow down cybercrimes. It can affect any one regardless of his or her race and religion. It can affect multiple countries within a split second. As such, combating cybercrimes needs a collective global effort and a comprehensive and cooperative strategies. Budapest Cybercrime Convention is a joint effort designed to address those prevalent issues by the Council of Europe and other State Parties. The Cybercrime Convention is the bastion and provides the strategic framework to combat cybercrimes effectively.

**Building up to this stage and our Cyber Crimes Act No 03 of 2021**

Prior to the enactment of the Fijian Cyber Crime Act, the only provisions available to tackle cyber offences were under Sections 336 to 346 of the Crimes Act 2009. Some procedural supports were also provided under the Criminal Procedure Act 2009 and the Prevention of Bribery Act, however, were of limited use due to lack of capacity to provide necessary support from the service providers and users. Nevertheless, it is noteworthy that the Commission, within a limited legal framework, had successfully investigated and prosecuted several large-scale corruption offences committed in tandem with cybercrimes. Two cases are worthy to note at this juncture.

The first case is *FICAC v Ana Laqere and others*. The case involved several officers of former Public Works Department (PWD) and some private companies. The officers were working in the Accounts section of its Central and Eastern Division office situated in Walubay and colluded with private company owners/directors to raise bogus procurement orders and managed to siphon out millions of dollars from PWD. They manipulated the Financial Management Information System (FMIS) to an unprecedented level in diverting public funds to those companies.

In addition, we also noted that the perpetrators were stealing the identity of some reputed companies and used those company quotation forms through forgery and committed some form of "identity theft".

All correspondence must be addressed to the Deputy Commissioner and sent to the FICAC Headquarters

Many reputed companies fell victim this scam. However, there was no specific offence existing at that point in time to tackle these complex scenarios. They all were charged under Crimes Act for abuse of Office and obtaining financial advantage.

All accused persons from PWD were convicted before the High Court and serving prison sentences and some cases are still pending before the court against private companies. When the investigations commenced, we realized that most of the physical documentary evidence relating to fake procurements were destroyed, however, we managed to reconstruct them using the FMIS data and information.

This is one of the first examples that the Commission realized the extent of the cybercrime activities occurring in corruption committed by public servants and the need to have a strong legal framework to battle corruption related cybercrimes.

The second example is the *FICAC v Villiame Katia* case where the former deputy official receiver squandered more than 4 million dollars from the Official Receiver's accounts. One of his modus operandi was to use the computer system available in the Official Receiver's Office to create fake debtors and creditors accounts and managed to convince his supervisors and the banks to make payments which he directly benefitted from.

As such, the cyber related corruption involving large sums of public money was becoming prevalent and there was a need to have a strong legal framework that is compatible with the international standards as stipulated in the Convention.

Fiji commenced preparatory work to enact a cybercrime legislation few years ago with stakeholder collaborations and also with the help of experts, consultants and representatives of the Council of Europe. I am very proud to say that the Commission engaged in this process and contributed well at every important stage in that process. At this stage, I must take this opportunity to acknowledge the contribution rendered by the then Consultant to the Government of Fiji, Mr Jayantha Fernando and his colleagues from the Bureau of the Cyber Crime Convention of the Council of Europe, without whose guidance, this journey would not have been possible.

Fast forward to the present day, we now have a Cybercrime Act ready. We also took part in the recent assessment undertaken by the Council of Europe and now eagerly waiting to make use of the provisions of the Act to strengthen our fight against corruption. As I said before, cybercrimes or use of internet and digital devices are a very common way of committing corruption offences and almost all of our investigations now have a cybercrime component. In this regard, Commission has established a specialized unit called "Digital Forensic Unit" with expert investigators in extracting digital evidence.

### **Salient features of the Cyber Crime Act**

The Cyber Crime Act comprehensively addresses the salient features of the Convention. The issues have been addressed under three key areas:

- Substantive Criminal Law including the legal definitions of important technological terms
- Procedural Law with reference to cyber crime investigations and collation of electronic evidence in relation to any crime
- International cooperation

It is not my endeavor to speak in detail about the features of the Cyber Crimes Act. However, as noted by our consultants and experts, we can proudly say that the Act is one of the robust statutes available hitherto in the Pacific region to combat cybercrimes. The Convention was considered as a reference model and incorporated various cybercriminal conducts under the domestic law as criminal offences. It provides procedural powers to investigate and prosecute cybercrimes and also safeguards the rights

of the public at large. The effective international cooperation among the stake holders of criminal justice is imperative as the cybercrimes often multi- jurisdictional.

#### **Human Rights and democracy strengthening**

In addition to the general measures safeguarding human rights, it effectively addresses women and children's rights as well. Women and children are often exploited viciously by cybercriminals. The Cybercrime Act provides sufficient tools to combat them effectively. Severe penalties imposed for child pornography is an example.

#### **Accession**

We strongly support Fiji's accession to the Convention. It will connect Fiji with the global efforts in fighting cybercrimes and will also provide several benefits. Fiji is a commercial hub in the South Pacific and it is important to provide a safe commercial platform for all parties involved in commercial activities by providing a safe cyber space. Women and children must feel safe in the cyber environment. Fiji can also benefit from international cooperation immensely through capacity building.



**Rashmi Aslam**  
Commissioner

3 October 2022



Fiji FIU's Submission:  
**Convention of Cybercrime- The Budapest Convention**

STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE

Monday 3 October 2022

RAZIM BUKSH  
DIRECTOR  
Fiji FIU

## Financial Intelligence Unit

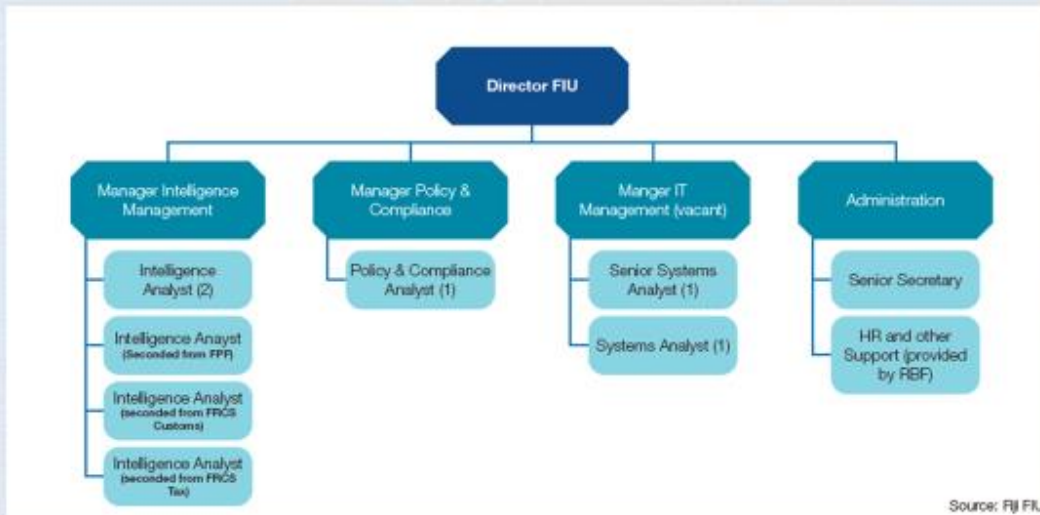


- Established in 2006 under Section 22 of the Financial Transaction Reporting Act (2004);
- An agency of the Fijian government;
- Administered & funded by Reserve Bank of Fiji;
- Our Vision: Protecting Fiji from Money Laundering;
- Administrative FIU, together with regulatory and enforcement functions; and
- Functions, duties and powers outlined in Section 25 of the FTR Act.



## Our Role

## FIU Organisation Structure



## Financial Institutions under FTR Act



**FijiFIU**

Fiji Financial Intelligence Unit



Sector	No. of Reporting Entities Registered for Online Reporting to the FIU
Commercial Banks	6
Foreign Exchange Dealers & Money Remitters	11
Mobile Phone Money Remitters	2
Finance Companies	12
Legal practitioners	51
Insurance & Superannuation	13
Accounting Firms	11
Securities and Brokers	3
Real Estate Agents	26
Money Lenders	1
Others	10
<b>TOTAL</b>	<b>146</b>

Source: Fiji FIU

## FIU's Intelligence Products Disseminated in 2021



Source: Fiji FIU

**418  
Intelligence  
Reports**

**952  
Individuals**

**384  
Businesses &  
Entities**



**FijiFIU**

Fiji Financial Intelligence Unit

## FIU's Intelligence Products Disseminated: 2017 - 2021

Fiji FIU - Value of CDRs to Law Enforcement Agencies					
Law Enforcement Agency	2017 (\$)	2018 (\$)	2019 (\$)	2020 (\$)	2021 (\$)
Fiji Revenue & Customs Service	220,041,608	114,060,337	12,175,316	54,216,419	46,959,343
Fiji Police Force	9,000,000	54,700,000	8,800,000	34,331,425	14,578,833
Immigration Department				6,707,064	8,913,246
FICAC		320,000		10,901,023	259,079
<b>Total</b>	<b>229,041,608</b>	<b>169,080,337</b>	<b>20,975,316</b>	<b>106,155,931</b>	<b>70,710,501</b>



**FijiFIU**

Fiji Financial Intelligence Unit

### FIU's Contribution to Combating Cybercrime

Cases Disseminated to Law Enforcement Agencies



**FijiFIU**

Fiji Financial Intelligence Unit

FIU continues to receive, analyze and disseminate cybercrime related cases on:

- ✓ Internet Banking Fraud - Unauthorized bank transfers;
- ✓ ATM Skimming;
- ✓ Email Spoofing;
- ✓ Business Email Compromise (BEC);
- ✓ Phishing / Spear Phishing;
- ✓ Identity Theft;
- ✓ Social Media Scams.

## FIU's Contribution to Combating Cybercrime

National Engagements



**FijiFIU**

Fiji Financial Intelligence Unit

### 2010 Fiji Cybersecurity Working Group

- Established in 2010, FIU is a member of Fiji's national cybersecurity working group on technical, legal and security issues;
- FIU was part of the working group meetings in 2016 as it deliberated on the formulation of national cyber security strategy;
- FIU also met with consultants on cybersecurity to discuss cybercrime legislations and cybersecurity strategy.

### 2016 National Cybersecurity Strategy

- Approved in 2016, FIU was part of the consultation, drafting and implementation process of the national cybersecurity strategy;
- Vision: To enable a secure, resilient and available Cyberspace that will enhance awareness & socio-economic development of all Fijians;
- Protect critical infrastructure, ICT and related services;
- Combat cybercrime and manage cyber threats;
- Enhance national safety and security in cyber space;
- Develop capability, legal framework and expertise in Cybersecurity;
- Promote Cybersecurity awareness, information sharing and collaboration;
- Enable secure use of Fiji's cyberspace for promotion of human rights & socio-economic development.

## FIU's Contribution to Combating Cybercrime

National Engagements



**FijiFIU**

Fiji Financial Intelligence Unit

### Cybercrime Act 2021

- FIU was part of the consultation and drafting of the cybercrime legislation and bill.
- Cybercrime Act 2021 adopts the 48 Articles of the Budapest Convention to address the following:
  - ✓ Offences against the confidentiality, integrity and availability of computer data and systems;
  - ✓ Unauthorised access to, and unauthorised interception of, computer systems or computer data;
  - ✓ Computer-related forgery;
  - ✓ Computer-related fraud;
  - ✓ Collection of electronic evidence;
  - ✓ International cooperation;
  - ✓ Investigation and prosecution of cybercrime related offences;
  - ✓ Preservation of stored computer data;
  - ✓ Extradition; and
  - ✓ Penalties.

## FIU's Contribution to Combating Cybercrime

International Engagements



**FijiFIU**

Fiji Financial Intelligence Unit



- FIU is a member of the Egmont Group of FIUs with a global network for sharing intelligence and international cooperation with 166 other FIUs;
- The Egmont Group provides FIUs with a platform to securely exchange expertise and financial intelligence to combat money laundering, terrorist financing (ML/TF), cybercrime and associated predicate offences;
- Foreign FIUs provide valuable due diligence when sharing intelligence which assists in uncovering highly sophisticated web of fraudulent transfers from Fiji bank account holders to beneficiaries from multiple jurisdictions holding the bank account details of the cybercriminals through the Egmont Secured Channels.



- Established in 2017, FIU is part of Pacific Cyber Security Network (PaCSON) in developing capacities which address cyber threats, strengthen cyber security and combat cybercrime;
- Australian Government Assistance;
- Other country members include Australia, Cook Islands, Kiribati, Marshall Islands, Nauru, New Zealand, Niue, Palau, Papua New Guinea, Samoa, Solomon Islands, Tokelau, Tonga, Tuvalu, Vanuatu, and USA;
- Not a CERT and does not provide Incident Response capability.

## FIU's Contribution to Combating Cybercrime

International Engagements



**FijiFIU**

Fiji Financial Intelligence Unit



- In 2017, FIU was part of the Fijian delegation to conduct onsite visit to Computer Emergency Response Team (CERT) Australia to gather insight on the functions and set-up of a national CERT;
- The scoping visit was to gauge Fiji's readiness and commitment to develop a national CERT for Fiji;
- Founded in 1993, is a non-profit organization that provides advice and solutions to cybersecurity threats and vulnerabilities.

## FIU's Contribution to Combating Cybercrime

International Engagements



**FijiFIU**

Fiji Financial Intelligence Unit



### 24/7 Network

The Council of Europe supports the functioning of the 24/7 Network established according to Article 35 of the Budapest Convention as a tool for expedited international cooperation on cybercrime and electronic evidence.

How does the Network function in practice and who are its members?

- **FIJI FIU** is the current focal contact point of:
- **G7 24/7 Cybercrime Network** since May 2018.
- Fiji was the 82<sup>nd</sup> country to join the worldwide network and it currently has 90 members.
- **Background**
  - The G7 24/7 Network was established as a result of the meeting of G8 Justice and Interior Ministers in December 1997.
  - The G7 24/7 points of contact is an informal network which assists with timely exchanges of critical information.

## FIU's Contribution to Combating Cybercrime

Cybercrime awareness and capacity building to Law Enforcement Agencies and Other Stakeholders



**FijiFIU**

Fiji Financial Intelligence Unit

Date	Cybercrime Awareness and Capacity Building
26 May 2010	Cyber Security Workshop
26-27 May 2011	MSG Police Regional Information Sharing Workshop on Cyber Security
19-21 November 2017	Fiji-Australia Cybersecurity Dialogue
2017-2019	Postgraduate Diploma in Cybersecurity
23-25 September 2018	2nd Fiji-Australia Cybersecurity Dialogue
30 October 2019	Workshop on Drafting and Application of Cybercrime Legislation
11 February 2020	Presentation on Cybersecurity Awareness during Safer Internet Day
13-14 February 2020	Multinational Communications Interoperability Program (MCIP) Cyber Services, Cyber Training
24-25 March 2021	Countering DPRK Cyber Threats: An Interactive Virtual Training for Financial Institutions in Fiji
13 May 2021	Pacific Cyber Week Webinar
28 July 2021	Cybersecurity Open Source Tools
31 August 2021	Digital Fiji Training on Developing a National CERT

## FIU's Contribution to Combating Cybercrime

Alert Notices Issued to Financial Institutions



**FijiFIU**

Fiji Financial Intelligence Unit

The FIU continues to engage with financial institutions to issue alert notices on emerging cyber criminal activities in Fiji.

Date	Alert Notice	Issued To
22 September 2011	Warning against email scams, cybercrime financial transactions and fraudulent international remittances.	Commercial banks and money remittance service providers
21 December 2012	Two named individuals involved in possible cybercrime offences.	Commercial banks and money remittance service Providers
27 March 2014	Possible advance fee fraud by Nigerian nationals	Commercial banks and money remittance service Providers
11 August 2014	Email spoofing for local businesses	Commercial Banks and Money Remittance Service Providers
5 November 2014	Computer virus targeted at ATMs	Commercial banks
30 January 2017	Possible advance fee fraud, lottery scam related remittances and email spoofing	Commercial banks and money remittance service Providers
15 May 2017	Financial institutions to take necessary preventive precautions against WannaCry Ransomware	Commercial Banks, Foreign Exchange Dealers, Finance Companies and Other Financial Institutions
29 June 2017	Alleged ATM and Credit Card Skimming	Commercial Banks, Foreign Exchange Dealers and Money Changers

## FIU's Contribution to Combating Cybercrime

National Awareness



**FijiFIU**

Fiji Financial Intelligence Unit

The FIU continues to inform and caution members of the public on emerging cyber criminal activities in Fiji by issuing press releases.

Date	Press Release	Cybercrime Offence
23 September 2011	Beware of Scam Emails and Cybercrime Financial Transactions.	Phishing
22 November 2011	Beware of Internet hacking and email scams	Email spoofing
15 June 2012	Authorities Tackle Cybercrime in Fiji	Internet Banking Fraud
17 April 2014	Beware of email spoofing (Impersonation)	Email spoofing
11 August 2015	Fiji completes national risk assessment on money laundering and terrorist financing	Cybercrime ranked Medium
18 March 2016	ATM Skimming in Fiji	ATM Skimming / Identity Theft
18 August 2016	Fake Facebook Accounts	Identify Theft
27 March 2020	COVID-19 related online scam	Social Media Scams

## What is Cyber Security?



FijiFIU

Fiji Financial Intelligence Unit



## The Fundamentals

Cyber Security is the practice of protecting organisations, individuals and networks from digital attacks and accidents that result in a **negative impact**.

Cyber Security addresses **threats** to our organisations and communities by implementing **controls** across **People, Process and Technology**.

- **People** – Citizens, colleagues, ourselves.
- **Process** – Methods to achieve our goals.
- **Technology** – Computers, systems, networks..

17

## Who They Are



FijiFIU

Fiji Financial Intelligence Unit

### Nation States & APTs

Advanced Persistent Threat

- Target private & public sectors.
- Seek strategic or intellectual property.
- Use a variety of sophisticated techniques.
- Motivated by economic, military, political or strategic gain.

### Competitors

- Target similar / peer businesses.
- Motivated by potential financial or market gains.
- Likely to outsource the attack to avoid attribution.

### Insiders

- Current or former employees.
- Have access to sensitive information.
- Motivated by financial gain, personal advantage or revenge.
- Can be malicious or unintentional.

### Hackers

- Motivated by ideological issues and social causes.
- Seek to cause reputational damage or disruption.
- Attacks range in sophistication.

### Organised Crime

- Motivated by financial gain or to finance criminal activities.
- Attempt to steal financial, credit card & sensitive data
- Common attacks methods include ransomware, spear phishing etc.

### Individuals 'Script Kiddies'

- Sophistication of attacks varies.
- Motivated by financial gain, fun and notoriety.
- Tools will also vary in sophistication.

## Data Breaches

*An incident where information is stolen or exfiltrated without knowledge or authorisation.*

### Types of information most often breached

Sensitive   Proprietary   Confidential   Financial   Personal



## Phishing

*An attack where messages appear to come from a trusted or reputable source, and aim to coax the victim into disclosing sensitive information*

### How?

- Email (traditionally)
- SMS (SMSishing)
- Over the phone (Vishing)
- From social media messages

### What to look for?

- Poor spelling or grammar
- Generic greetings/titles
- Unusual or misspelt addresses
- Unusual attachments or links

### What to do?

- Avoid clicking links / files
- Verbally verify requests
- Avoid sharing information publicly
- Use a spam filter
- Provide information via trusted means

## Business Email Compromise (BEC)



**FijiFIU**

Fiji Financial Intelligence Unit

- Targets key individuals within an organisation, using legitimate emails and contacts to take advantage of business processes for financial or material gain.
- BECs typically target mid-level executives or financial officers.
- Often have an urgent timing imperative and come from a position of power.
- Are sent from a legitimate email, and may take place in stages or come mid-conversation



## BEC- Themes



**FijiFIU**

Fiji Financial Intelligence Unit

### Vendor Invoice / Payment

**Subject(s):**  
'Urgent',  
Assistance needed,  
Request Available?  
'Invoice payment '

Scammer impersonates CEO or CFO & asks Finance to urgently send a payment to a vendor or other party.

### Gift Cards

**Subject(s)**  
'Need your help'  
'Quick Task'  
'Favor'

Impersonate manager & asks to purchase gift cards, take a photo and send the image. Scammer redeems the cards.

### Payroll Exchange

**Subject(s):**  
Payroll Update  
Direct Deposit  
Update/Change  
Change in bank info

Scammer impersonates an employee and asks HR staff to change the bank account for salary deposits.

### Phone Number

**Subject(s):** Hello  
[person]  
Quick Request

Scammer impersonates CEO, CFO or manager & asks employee for cell phone number, from where a text message occurs.

### Altered Invoice

**Subject(s):**  
Varies according to  
actual email  
correspondence /  
project type.

Scammer gets access to email, monitors email looking for invoices or transactions about to happen, then injects themselves in the conversation & alters invoice.

## Ransomware

*A malicious form of software that blocks or limits access to your computer or information until a ransom is paid.*

Ransomware spreads to a network through malicious files, websites and advertisements.

**Payment DOES NOT guarantee data**



- Up-to-date systems / patches
- MFA on accounts, systems & devices
- Regular back ups (and test restoration)



## Malware

*Software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system.*

**Common signs of Malware:**



Loading...



**Prevention:**

- Up to date anti-malware software
- Only visit/download from trusted sites
- Be wary of links/files
- Firewalls

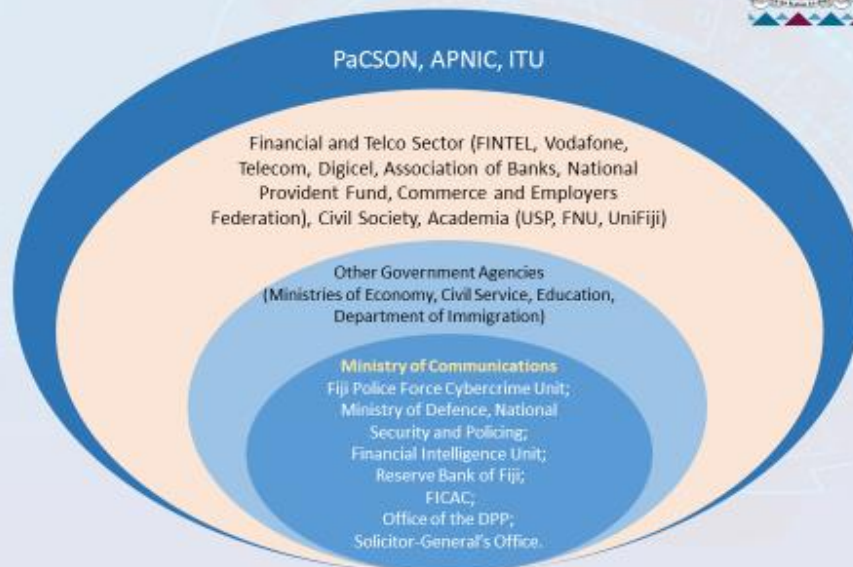
25

## Key Cyber Security Stakeholders in Fiji



**FijiFIU**

Fiji Financial Intelligence Unit



## Challenges Dealing with Cybercrime



**FijiFIU**

Fiji Financial Intelligence Unit

- Cyber criminals operating anonymously outside of Fiji and from multiple jurisdictions.
- Recovery of stolen funds and proceeds of crime from cybercrime related offences.
- Acquiring, handling and storing of digital evidence to build a cybercrime case.
- Gaps in the legal framework to prosecute cybercrime related offenses.
- Extradition of cyber criminals to be trialed for the cybercrime offences in the country of offence committed.
- Lack of resources, expertise and budget to analyze all cybercrime related offences (data science, artificial intelligence, bulk data analytics, etc).

## Impact of Convention on Cybercrime



**FijiFIU**

Fiji Financial Intelligence Unit

- The following cybercrime related offences are covered under Article 2 – 8, 10 of the convention:
  - ✓ Internet Banking Fraud - Unauthorized bank transfers;
  - ✓ ATM Skimming;
  - ✓ Email Spoofing;
  - ✓ Business Email Compromise (BEC);
  - ✓ Phishing / Spear Phishing;
  - ✓ Identity Theft;
  - ✓ Social Media Scams.
- Article 24 allows extradition between member countries to prosecute cyber criminals operating outside of Fiji and in multiple jurisdiction.

## Recommendations



**FijiFIU**

Fiji Financial Intelligence Unit

- FIU fully supports the proposed convention on cybercrime as it addresses key gaps in relation to cybercrime offences under the current Fijian Government legal framework;
- Gaps in the government cybercrime regulations and controls allow opportunities for cybercriminals to see Fiji as a potential haven to commit cybercrimes and exploit Fiji's financial system.
- The convention addresses the following gaps in relations to cybercrime related offences:
  - ✓ Offences against the confidentiality, integrity and availability of computer data and systems;
  - ✓ Unauthorised access to, and unauthorised interception of, computer systems or computer data;
  - ✓ Computer-related forgery;
  - ✓ Computer-related fraud;
  - ✓ Collection of electronic evidence;
  - ✓ International cooperation;
  - ✓ Investigation and prosecution of cybercrime related offences;
  - ✓ Preservation of stored computer data;
  - ✓ Extradition; and
  - ✓ Penalties.



## CASE STUDY 1

- A 44 year old man was reported to the FIU for conducting deposit transactions totaling \$2 million in a three year period.
- We established that he had \$4.4 million in investments and bank accounts.
- The individual is a director of two local companies.
- Bank account analysis showed that the funds in his investment and bank accounts were sourced from the business with various narrations such as “Profit from Business”.
- We identified a **discrepancy of \$8.2 million** between deposits observed through his business and investment accounts and his taxable income.

## CASE STUDY 2



**FijiFIU**

Fiji Financial Intelligence Unit

- In 2020, a night club deposited \$30,000 in cash into its bank account.
- The owner operates the night club as a sole proprietorship.
- In 2020 and 2021, the night club received **\$3.9 million** in large cash deposits.
- It is unclear how the night club generated these funds given the Covid-19 restrictions that were in place in 2020 and 2021.

## CASE STUDY 3



**FijiFIU**

Fiji Financial Intelligence Unit

- A 26 year old was receiving large cash deposits into his bank account totaling more than \$500,000 in a three year period. The deposits were apparently farm income. He also owned a freehold property.
- Spending patterns through his bank account indicated that he lived in a different area from where the alleged farm was located. Cash deposits were also done by a third party. A *power of attorney* over the account was identified.
- 3 other individuals were identified with similar patterns in their bank accounts.
- They had conducted large cash deposits of \$5 million in 3 years and acquired various freehold properties.

## Other Case Studies – Abstracts!



**FijiFIU**

Fiji Financial Intelligence Unit

1. An individual on the social pension scheme had **37 land titles** registered under his name.
2. A foreigner on a visitors permit was found in possession of prohibited sea products. He owned three vehicles and paid his fine with cash. He **does not have any bank accounts** and it is unclear how he paid for and acquired the vehicles.
3. A **minor** received an international remittance of \$150,000 from a **foreign entity**.
4. An individual received multiple high value international money transfers from unknown third parties in a span of **9 days**.

## Other Case Studies – Synopsis!



**FijiFIU**

Fiji Financial Intelligence Unit

5. In 5 months, a individual received multiple **deposits from third parties** totaling \$250,000.
6. A person brought \$40,000 in **cash** as a deposit **to purchase property**. The funds were not obtained from a bank account.
7. **Massage parlor** received **\$567,000** in cash deposits followed by subsequent cheque withdrawals over a 12 month period.
8. An individual purchased an **investment product with \$150,000 in cash**.
9. An individual opened an account and in a span of 2 months he made **20 cash deposits** ranging from \$9,200 to \$9,900 totalling approx. \$200K.

## Other Case Studies – Synopsis!



**FijiFIU**

Fiji Financial Intelligence Unit

5. In 5 months, a individual received multiple **deposits from third parties** totaling \$250,000.
6. A person brought \$40,000 in **cash** as a deposit **to purchase property**. The funds were not obtained from a bank account.
7. **Massage parlor** received **\$567,000** in cash deposits followed by subsequent cheque withdrawals over a 12 month period.
8. An individual purchased an **investment product with \$150,000 in cash**.
9. An individual opened an account and in a span of 2 months he made **20 cash deposits** ranging from \$9,200 to \$9,900 totalling approx. \$200K.

## Other Case Studies – Synopsis!



**FijiFIU**

Fiji Financial Intelligence Unit

13. An individual would conduct monthly deposits into his **4 children's** accounts. Collectively he would deposit between \$10,000 to \$20,000 monthly. He withdrew \$300,000.00 collectively from the accounts and transferred the funds to his **another bank account**.
14. A **public service officer** acquired a taxi permit without paying for it. He and his wife collectively own 4 **high value vehicles**. He owns a **freehold property** in the Central division and made significant improvements in the last few years. They frequently **travelled abroad** and their children attended private school. The individual's transactions and accumulation of wealth were not consistent with the annual income declared.

## Other Case Studies – Synopsis!



**FijiFIU**

Fiji Financial Intelligence Unit

15. An individual conducted multiple transfers to other individuals. The total **cash/cheque deposits** amounted to more than \$900,000 in one year. The source of the cash deposits could not be determined.
16. PEP deposited \$17,000 cash into his personal account, believed to be **business proceeds**.
17. An individual received \$140,000 in remittances in one month. She claimed it was from her brother-in-law to build a house. The sender was also remitting funds to a **person of interest** to law enforcement.
18. An individual working at a financial institution provided a loan of \$1.5 million to an entity.

## Other Case Studies – Synopsis!



**FijiFIU**

Fiji Financial Intelligence Unit

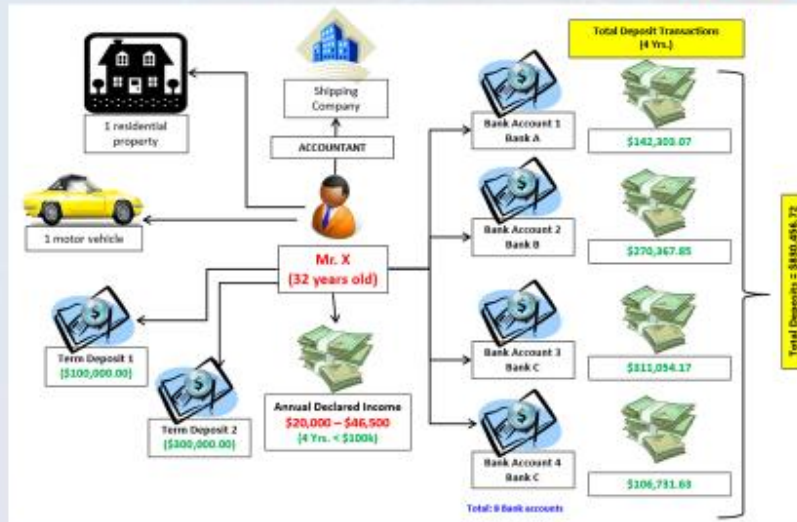
19. A middle-aged female in the USA sends several remittances within a few months totalling \$1.2million to several young females in Fiji.

## Case Study 20 – Suspicious Accountant



**FijiFIU**

Fiji Financial Intelligence Unit

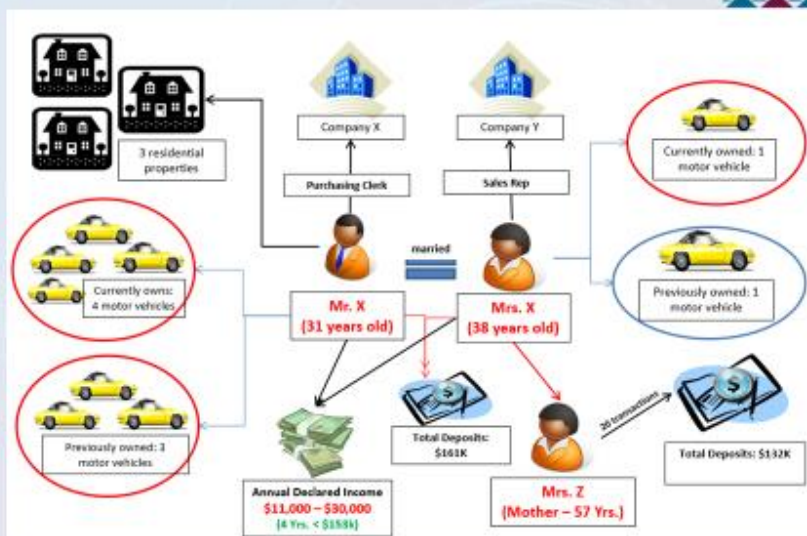


## Case Study 21 – Suspicious Clerk

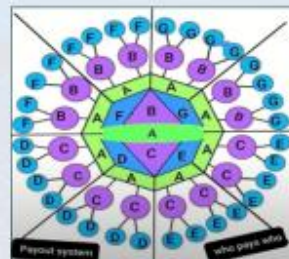


**FijiFIU**

Fiji Financial Intelligence Unit



## PYRAMID SCHEMES



- **Gifting Circle/Club:** (you would gift cash in exchange of more cash from other individuals. The more individuals join the club, the more cash is gifted to you)
- **Blessing Circle:** (you would bless another individual with cash and you cash blessing)
- **Commitment Circle:** (individuals make commitment (sell a vision, mission purpose of live)
- **Empowerment Lotus/Circle/Club:** (more geared to women)

In one month alone, the FIU identified more than 150 potential victims of the alleged illegal scheme that conducted over 300 deposit transactions totalling \$9,000



**FijiFIU**

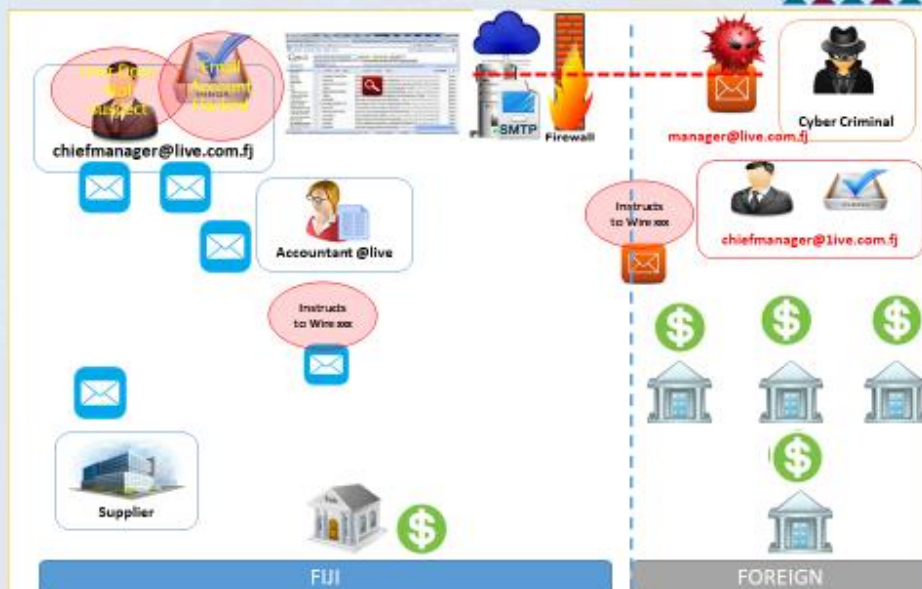
Fiji Financial Intelligence Unit

## Business Email Compromise



**FijiFIU**

Fiji Financial Intelligence Unit



## Email Compromise and Email Spoofing

2016 - 2022

**32 Incidents**

**More than \$6.4 million lost**

27 Entities



5 Individuals



### Top 3 Destinations

1. Hong Kong
2. USA
3. Australia



**FijiFIU**

Fiji Financial Intelligence Unit

## Email Compromise and Email Spoofing

- Commercial banks, financial institutions, businesses and members of the public are continuously advised by the Fiji FIU to exercise caution when handling email payment instructions for import trade transactions and large value personal **outbound foreign remittance transactions**.
- The Fiji FIU has received two reports resulting in losses totalling more than \$400,000 in the first two months of 2022.



**FijiFIU**

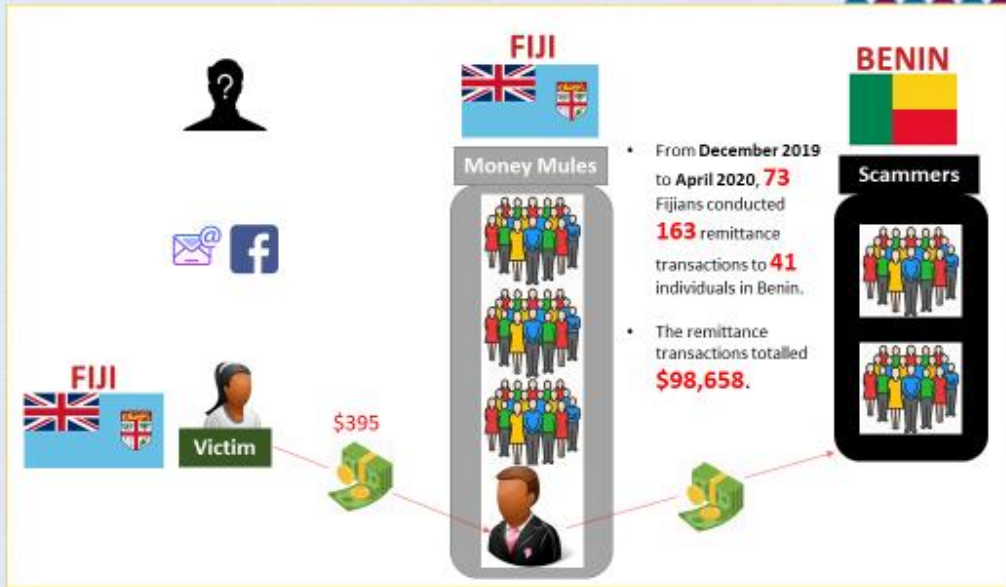
Fiji Financial Intelligence Unit

## Cyber Loan Scam

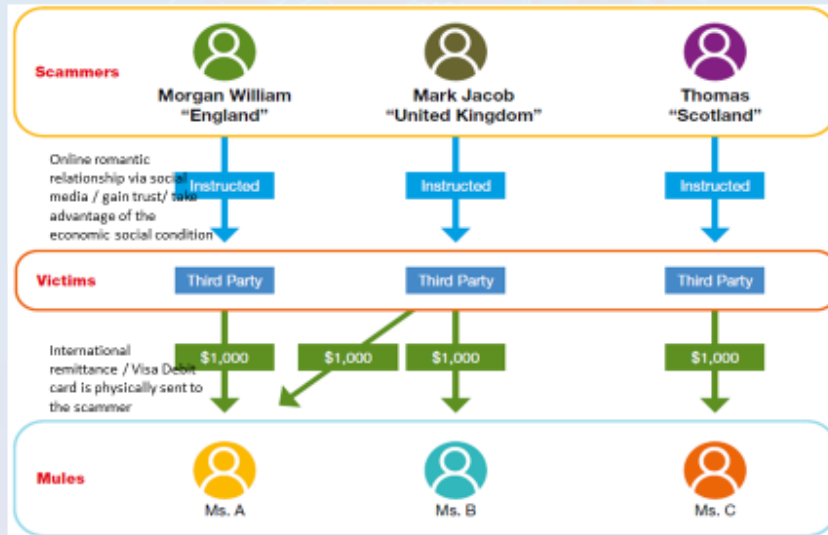


FijiFIU

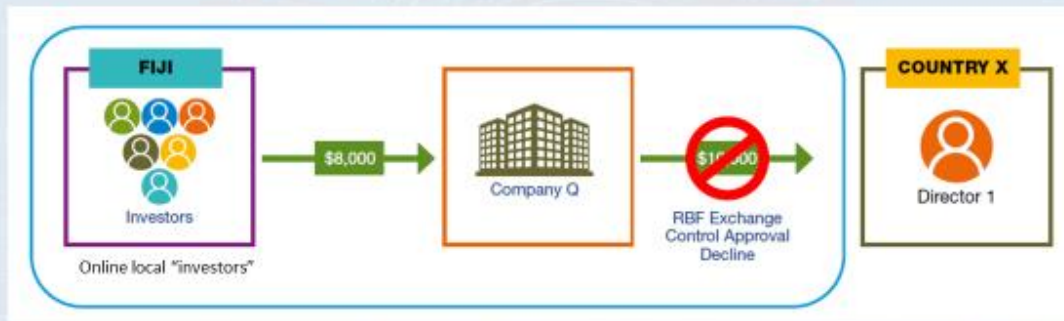
Fiji Financial Intelligence Unit



## Romance/Parcel Scam



## Cryptocurrency Trading



## Tax Evasion



## ATM Skimming

- 62 transactions of ATM withdrawals.
- Obtaining property by deception, attempt to obtain property by deception and possession of property suspected of being proceeds of crime.
- Found with fraudulent credit cards, fraudulent plastic cards, credit card reader and write machine, laptops, and USBs containing credit card and PIN numbers.
- Also found with more than \$200,000 in cash.
- CCTV footage showed the respondents involved in suspicious transactions at various BSP ATM outlets.

## ATM Skimming cont.

- Acquitted of obtaining property by deception and attempt to obtain property by deception.
- Guilty for the possession of property suspected of being proceeds of crime.
- \$203,011.00 was forfeited to the State.



## CONCLUSION



VINAKA VAKALEVU

[www.fijifiu.gov.fj](http://www.fijifiu.gov.fj)



**FijiFIU**

**Fiji Financial Intelligence Unit**

## **SUBMISSION BY THE CITIZENS' CONSTITUTIONAL FORUM**

### **PARLIAMENTARY STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE**

#### **CONVENTION ON CYBERCRIME (BUDAPEST CONVENTION)**

**Monday, 03 October 2022**

## **INTRODUCTION**

The Chairperson Honourable Alexander O'Connor and Honourable Members of the Parliamentary Standing Committee on Foreign Affairs and Defence.

The Citizens' Constitutional Forum (CCF) thanks the Standing Committee for the opportunity herein to provide a submission on the **Convention on Cybercrime** also known as the Budapest Convention ("the Convention"). The CCF is a non-governmental organisation based in Suva over more than 20 years' experience in education and advocacy on human rights, democracy, good governance, transparency and accountability, rights as reflected in the Bill of Rights in Fiji's 2013 Constitution and multiculturalism.

The CCF acknowledges the purpose and positive impact of becoming a Party to the Convention however there are a number of recommendations that the CCF believes needs highlighting before becoming a party to the Convention.

### **KEY POINTS ON THE CONVENTION ON CYBERCRIME**

#### **1. The Definition of Fundamental Human Rights**

Freedom of expression and right to privacy are fundamental human rights that are recognized under the 2013 Constitution of the Republic of Fiji and the ratified international conventions. Section 24 of the 2013 Constitution of the Republic of Fiji provides for the right to privacy which includes:

- Confidentiality of personal information;
- Confidentiality of communications; and
- Respect for private and family life

Article 15 of the Convention requires Parties to uphold the protection of human rights under domestic laws and international conventions such as the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms and the United Nations International Covenant on Civil and Political Rights (ICCPR). Fiji is a party to the ICCPR.

The definition and recognition of the right to privacy is stated in Article 17 of the ICCPR and Article 8 of the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms. Freedom of expression is covered under Article 19 of the ICCPR and Article 10 under the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms.

While these fundamental rights are defined and recognized under the two international instruments, CCF notes that these definitions are not specifically defined within the context of cyber crime i.e. there is no specific definition for privacy and what constitutes freedom of expression. CCF also notes that the current domestic legislation, the Cybercrime Act 2021 does not define these terms. Ambiguous cybercrime laws can give rise to its abuse as the interpretation of its provisions will be dependent on those who are enforcing it.

## 2. Balancing Human Rights and Power of National Security

Limitations to any human right must be done so in accordance with the principle of proportionality. This is also stated in Article 15 of the Convention. The principle of proportionality requires that any interference of rights must be proportionate with the legitimate reason for limiting it<sup>2</sup>.

Furthermore, matters of public interest change over time due to technological developments and societal attitudes. CCF submits that knowing what constitutes public interest within a law is essential in protecting human rights as well as ensuring good governance, transparency and accountability of the State and law enforcement agencies.

CCF submits that proper safeguards must be incorporated to ensure that acts or information which invades or restricts the right to privacy and freedom of expression without legitimate cause and proportionality does not take place. This should also be done in domestic legislation without delay.

CCF urges government to be mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy.

## RECOMMENDATIONS

In light of the above issues, the CCF submits that the following recommendations be considered:

- i. There must be specific definitions of privacy and freedom of expression within the context of cybercrime. Domestic legislation such as the Cybercrimes Act 2021 needs to be reviewed to define privacy as well as state what constitutes freedom of expression and public interest;

---

<sup>2</sup> <https://www.icj.org/chapter-5-standards-and-techniques-of-review-in-domestic-adjudication-of-esc-rights-2/5-4proportionality/> [Accessed: 30 September 2020]

- ii. Proper safeguards must be incorporated into the Convention and domestic legislation to protect fundamental human rights, avoid its misuse and encourage transparency and accountability ; iii. The need for guiding principles for the appropriate and accurate application and implementation of the same to ensure that citizens' fundamental human rights and freedoms which are enshrined in Fiji's 2013 Constitution are not violated;
- iv. Government to prioritize inclusive public consultations, given Fiji's diversity. Conducting meaningful engagement and collaborative work with local communities, civil society organisations and a wide range of stakeholders in addressing societal and cultural norms that pose barriers is needed during national processes of drafting and implementation of new policies and laws; and
- v. Monitoring, development and/or revision of frameworks in support of the implementation of the convention (subject to the protection of human rights) and any relevant recommendations received from state and non-state actors must be genuinely considered and reflected locally without impractical delay.

Salanieta Tamanikaiwaimaro

London

England

**United Kingdom**

The Chairperson

Standing Committee on Foreign Affairs and Defence

P.O.Box 2532

Government Buildings

Suva

**Fiji**

**Re: Submissions on the ETS 185 – Cybercrime Convention, 23.XI.2001**

Esteemed Members of the Standing Committee on Foreign Affairs and Defence:

- Chair Hon. Alexander O'Connor - FijiFirst Party, Government MP;
  - D/Chair Hon. Dr Salik Govind- FijiFirst Party, Government MP;
  - Hon. Selai Adimaitoga- FijiFirst Party, Government MP;
  - Hon. Peceli Vosanibola- SODELPA Party; Opposition MP;
  - Hon. Lenora Qereqeretabua- NFP Party; Opposition Party
1. Mr Chairman, Hon.Alexander O’ Connor thank you for the privilege and opportunity to participate in the dialogue and in your deliberations. I seek leave to submit my written submissions following my verbal submissions so as to assist you in your deliberations.
  2. As the Esteemed Standing Committee deliberates on the elaborate submissions made by the public and on the invitation by the Council of Europe to be a part of ETS 185 – Cybercrime Convention, 23.XI.2001 (“Budapest Convention”), it is important that we take the panoramic view and also seek to understand the context of the International Instrument, the lay of the land of the Republic of Fiji and of course the substantive domestic law.
  3. My submissions will take the following course:

- a. Context
- b. International Law
- c. Deficiencies and Lacunas
- d. Capacity and Readiness

## Context

4. Context is very important as it shapes meaning.
5. As we are looking at the context it is also important to review, assess these through the following tools:
  - a. Economic and financial;
  - b. Socio-cultural;
  - c. Infrastructure;
  - d. Legal;
  - e. Technology.
6. It is also important that when looking at the whether Fiji decides to accept the Council of Europe's invitation to accede to the ETS 185 – Cybercrime Convention, 23.XI.2001 ("Budapest Convention") that it looks at the following pillars:
  - a. Context of the Budapest Convention;
  - b. Context of the Republic of Fiji;

### *Context of the Budapest Convention*

7. The context in which the text of the international instrument was negotiated is canvassed within "The Special Edition Budapest Convention 2022", a 137 page comprehensive document outlying its context.
8. Issues of harmonization of laws surfaced in as early as 1983 when the "Organisation for Economic Cooperation and Development (OECD) undertook a study to determine whether it was possible to have international harmonization of criminal laws around computer crime and abuse"(pg.15 The Special Edition Budapest Convention 2022).
9. This led to the 1986 Report<sup>3</sup> which "*surveyed existing national laws for a number of states and recommended a **minimum list of abuses** that States should consider prohibiting by criminal sanction for example:*
  - a. *computer fraud and forgery,*
  - b. *alteration of computer programmes and data, and*

---

<sup>3</sup> OECD (1986), Computer-related crime: analysis of legal policy, Paris.

- c. *interception of computer functions and communications*” (ibid).
10. A majority of the committee members also recommended the inclusion of other abuses, such as theft of trade secrets and unauthorised access to, or use of, computer systems. In the same year and inspired by the work” (ibid).
11. According to the Special Edition Budapest Convention (pg 16), the same year, which was 1986, the Council of Europe inspired by the work of the OECD, the

---

Council of Europe initiated a study with a view to developing guidelines to assist legislators to determine which computer abuses should be criminalized, and how to define such having regard to the need for protection of both computer systems and civil liberties and its report<sup>4</sup> added to the OECD list what it thought should be criminalized which include the following:

- a. unauthorised access to and interception of computer systems;
  - b. damage to computer data or programmes;
  - c. unauthorised reproduction of computer programmes;
  - d. alteration of data or programmes
  - e. unauthorised use of a computer.
12. The Council of Europe Report also addressed “privacy protection, victims, prevention, extraterritorial jurisdiction and procedural issues such as search and seizure, interception of communications and international cooperation” (ibid).
13. The Special Edition Budapest Convention gives a comprehensive framework for how these minimum offences were drafted and how they were subsequently referred to and referenced by drafters and negotiated by the countries involved in negotiating the text and the key thing to pick out is that the minimum offences were picked by a handful of people in the 1980s which led to two key recommendations:
- a. Recommendation No.R (89) on computer related crime that is substantive criminal law which was adopted in 1989;
  - b. Recommendation No. R (95) concerning problems of criminal procedural law connected with it, was adopted in 1995.
14. That in 1997 the drafting of the Budapest Convention began before it became a Convention in 2001.
15. So historically, the minimum offences had its root from the 1986 OECD Report and so you will see that much of the language is confined to the word “computer” as opposed to the word “cyber”.

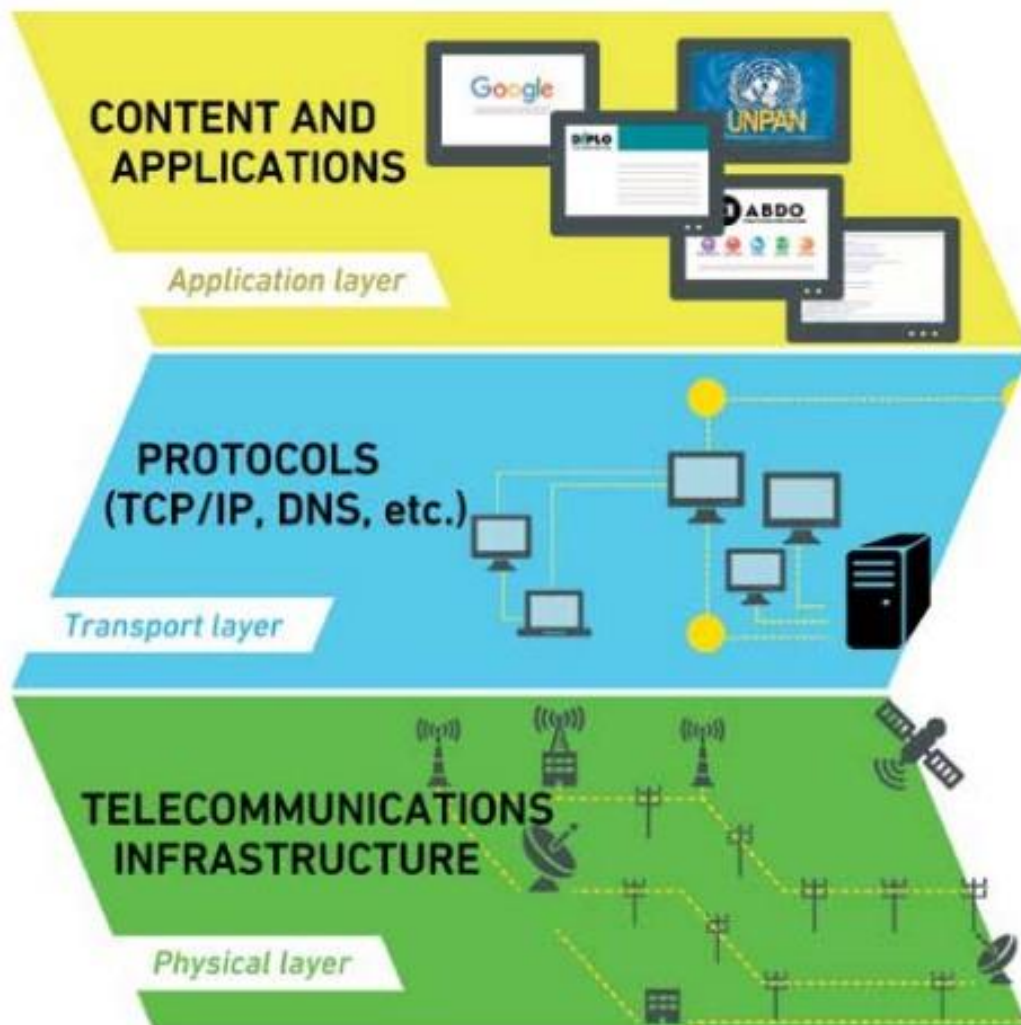
---

<sup>4</sup> Council of Europe (1990), Computer-related crime: Recommendation No. R (89) 9 on computer-related crime and Final Report of the European Committee on Crime Problems, Strasbourg.

16. To be fair those that commissioned those early studies did a sterling job which obviously resulted in studies and reports that led to recommendations but it is important to understand that the environment as we know it has drastically changed.
17. More importantly to understand the offences, it is also important to understand what the cyber environment means.
18. To this end, I would submit the following illustration to show the landscape of what a cyber environment is.

---

Figure 1 Illustration of Internet Layers or the Cyber environment



19. The drafters when drafting the Cyber Crime Act 2021 literally superimposed 90% of the Budapest Convention, see Annexure 1 and much of which inherits drafting text that is at best “archaic and an old dress”.
20. This is not to say that the minimum offences listed are not relevant but that the drafters since those studies were commissioned prepared what was relevant in then and had clearly when those that negotiated the final text did they still based it on the rudimentary foundational outcomes from the OECD and Council of Europe Studies.
21. The landscape since then has changed drastically since the 1980s and increasing reliance online and increasing activities happening within the cyber environment and it is important to look at the three layers of the internet when considering the cyber environment although arguably, they are interchangeable.
22. The Budapest Convention is brilliant in terms of how it has enabled and allowed countries that are a party to engage in mutual cooperation and as far as Fiji is concerned, it has already passed the Cybercrime Act 2021 which already allows Fiji to engage at its will and pace.

#### *Context of the Republic of Fiji*

23. In a sense, legislators or Parliamentarians act as a watchman of a nation and hold a sacred and divine duty where the fate of the nation is in its hands. This means that it requires wisdom to sift through public submissions and to take a step back and to assess what would best fit and best suit a nation.
24. In making that decision, it has to consider the following:
  - a. Economic and financial;
  - b. Socio-cultural;
  - c. Infrastructure;
  - d. Legal;
  - e. Technology.
25. In acceding to the Budapest Convention, questions that the esteemed Standing Committee can ask are as follows:
  - a. What is the economic impact and financial implication?
  - b. What is the socio-cultural implication?
  - c. What is the impact on our infrastructure?
  - d. What is the impact on our legal system and criminal justice system?
  - e. What is the technological impact?

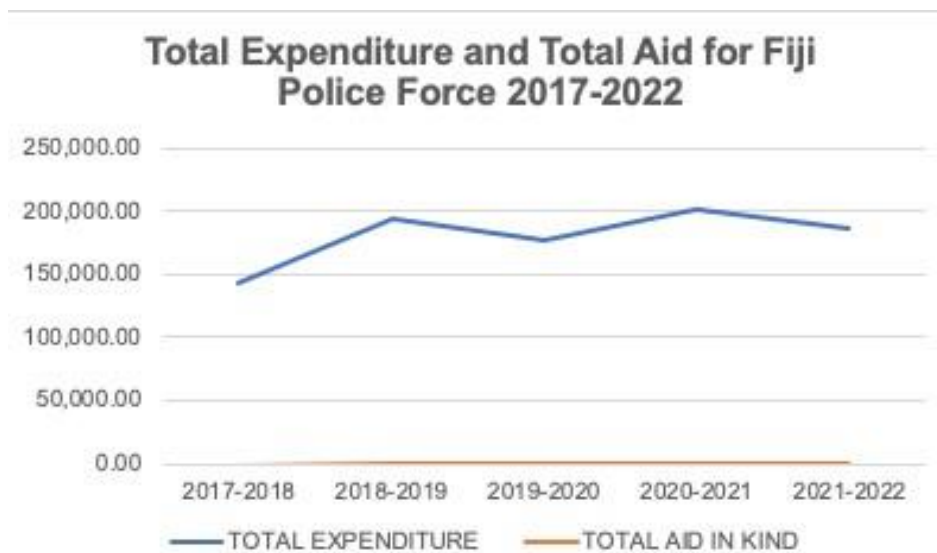
## Economic Impact

26. There are 67 parties to the Budapest Convention and imagine a case scenario where their countries Department of Justices are sending multiple requests at any one time. Who bears that cost?
27. To this end, I would refer you to review the budgetary allocation to the Fiji Police Force, Solicitor General's Office, Office of the Director of Public Prosecutor and Judiciary.
28. However for this exercise, we will select just one stakeholder which is the investigative arm which in this case is the Fiji Police Force of which the Cyber Crime Unit is a part of. See below:

**Table Showing Government Budget Estimates for the Fiji Police Force**

	<i>Actual</i>	<i>Estimate</i>	<i>Estimate</i>	<i>Revised Estimate</i>	<i>Revised Estimate</i>
	<b>2017-2018</b>	<b>2018-2019</b>	<b>2019-2020</b>	<b>2020-2021</b>	<b>2021-2022</b>
Established Staff	112,433.40	142,301.00	144,459.30	136,966.40	134,649.20
Government Wage Earners	1,072.10	1,021.10	1,021.10	1,203.90	1,188.50
Travel and Communications	6,107.70	5,583.00	5,038.00	3,958	4433.5
Maintenance and Operations	7,949.90	7,669.00	7,257.10	6,673.10	8857
Purchase of Goods and Services	4,684.20	5,664.00	4,781.00	3,043.50	2810.2
Operating Grants and Transfers	38.5	90.00	50	50	50
Special Expenditures	1,051.10	3,274.60	1,698.00	1,765.20	1,944.00
<b>TOTAL OPERATING</b>	<b>133,337.00</b>	<b>165,602.80</b>	<b>164,304.60</b>	<b>153,660.10</b>	<b>153,932.40</b>
Capital Construction	3,148.00	19,256.90	7,900.00	40,150.00	26,000.00
Capital Purchase	4,297.80	4,515.00	2,925.20	1,650	1,755.00
Capital Grants and Transfers	0	0	0	0	0
<b>TOTAL CAPITAL</b>	<b>7,445.80</b>	<b>23,771.90</b>	<b>10,825.20</b>	<b>41,800.00</b>	<b>27,755.00</b>
Value Added Tax	<b>2,361.80</b>	<b>4,135.20</b>	<b>2,659.60</b>	<b>5,151.60</b>	<b>4,122.00</b>
<b>TOTAL EXPENDITURE</b>	<b>143,144.60</b>	<b>193,509.90</b>	<b>177,789.40</b>	<b>200,611.70</b>	<b>185,809.30</b>
<b>TOTAL AID IN KIND</b>	<b>0</b>	<b>25</b>	<b>50.2</b>	<b>740</b>	<b>677.8</b>

29. From this, one can observe how the budgetary allocations by government are pretty much within the same range. See graph below:



30. Figures sourced from Fiji Government Budget Estimates and as you can see total aid is negligible compared to the total capital expenditure and operational expenditure that the Fiji Police Force has.

#### Infrastructure

31. For the entire system to work it will require the capacity development of all infrastructure and elements of the criminal justice system.

32. It requires legislators to be prophetic or futuristic as they see the future and prepare infrastructure to meet the demands of what is coming.

33. The Fiji Police Force in its submission to this esteemed committee mentioned that the Cyber Crime Unit has 11 staff including IT officers which in my view is not enough to deal with the demand.

34. It will cost money to train investigators and build the human resource capacity to cater for the local context as well as the demands to come when engaged in mutual cooperation with the 67 nations that are a party to the Budapest convention.

35. It will also require high levels of infrastructure that will cause them to do their jobs well and access to resources and also safe means of preserving all forms of digital evidence to ensure that it is not corrupted and inadmissible in court.
36. These chain of evidence and also the mechanisms in which they are preserved are critical and also cost money to implement.
37. Kindly note that we have not touched on the avalanche of production orders and requests for mutual cooperation that would come and whether our local law enforcement officers have the bandwidth and capacity to cater for these issues.
38. As you can imagine the same has to be said for all elements of the criminal justice system which include judicial capacity, prosecutorial capacity and my view is that it requires a specialized court to address cybercrime and cyber security issues.
39. A highly skilled and specialised workforce costs money and will also need resources to be able to do their jobs well.

#### Sociocultural

40. What is the impact on global public interest or on the citizens of the Republic of Fiji?
41. For this reason, it should be encouraged that studies are commissioned to look into this.
42. Fiji has finite resources, and from the budgetary allocations one can see that a level of stewardship is required which is why it is incumbent to factor into the planning process how the economic impact affects other budgetary allocations to other deserving ministries whether it is in setting up appropriate health care centers in rural Fiji, or underserved communities and those that are struggling such as single mothers.

#### Technology

43. When we discussed the context of laws and how the minimum offences were based on studies that were commissioned by OECD and the Council of Europe in the 1980s, I had also referred to the dress principle or fabric.
44. If you take old wineskin and patch it with the new, it will burst.
45. Whilst the laws can be technology neutral, the cyber environment has to be framed within Fiji's domestic laws primarily and whilst to some extent it is but there still needs to be a robust review of all policies and regulatory frameworks as these indirectly impact the chain of evidence and as I was making my submissions, I had used the example of "timestamping".
46. It would be such a shame when so much time is spent on investigating and gathering evidence only to have these thrown out because of anomalies and lacunas in the system which exist.

#### The Law

47. You will see from the Special Edition of the Budapest Convention (137 pages) that it paints the historical context of how the context was negotiated and also the various reports that were precursors to the drafting.
48. The Standing Committee has before it the following:
- ETS 185 – Cybercrime Convention, 23.XI.2001 which Fiji has been invited to accede to.
  - ETS189 - Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of racist and xenophobic nature committed through computer systems
  - CTS No. 224 Second Additional Protocol on Enhanced Cooperation and Disclosure of Electronic Evidence
49. As discussed whilst the Budapest Convention was drafted back then, at the time it was not comprehensive as evidenced by the Additional Protocols.
50. This is normal as when things progress, people are then able to see what the gaps are and to be able to create instruments to address it.

### *Capacity and Readiness*

51. Is Fiji ready to accede to the Budapest Convention?
52. It already has 90% of the Budapest text in its Cybercrime Act 2021 which was in my view back to front and a rush job where whilst we looked like we created new law, we literally took text from the 80s and passed it into law.
53. My personal view is that the Solicitor General's Office or the Standing Committee should commission Studies and reports just as they do in Europe to comprehensively look at what the existing framework is in 2022 in Fiji and then begin to create appropriate legal framework from there.
54. Mr Chairman O' Connor and esteemed members of the Standing Committee on Defence and Foreign Affairs, as you deliberate and review all the submissions, the nation of Fiji is counting on you to assess whether Fiji is ready.
55. Below are my recommendations.
- **Recommendation 1** – To not rush into acceding to the Budapest Convention
  - **Recommendation 2** – To commission studies posing specific questions pertaining to capacity and readiness and harmonization of domestic laws, economic and financial implications, criminal justice infrastructure with a view to highlight lacunas and solutions

Yours sincerely,

Zoe Angel formerly Salanieta Tamanikaiwaimaro

## **ANNEXURE 1**

**Table showing Comparison of Cyber Crime Act 2021 and Convention on  
Cybercrime Budapest, 23. XI.2001**

<b>Cyber Crime Act 2021</b>	<b>Convention on Cybercrime Budapest, 23. XI.2001</b>
s.1 Short title and commencement	
s.2 Interpretation	
s.3 Application	
s.4 Savings of certain laws	
s.5 Unauthorised access to computer systems	Article 2 - Illegal Access
s.6 Unauthorised interception of computer data or computer systems	Article 3 - Illegal Interception
s.7 Unauthorised acts in relation to computer data or computer systems	Articles 4 - Data Interference; Article 5-System Interference
s.8 Unlawful supply or possession of computer system or other device, or computer data or computer program	Article 6 - Misuse of Devices
s.9 Computer-related forgery	Article 7- Computer related Forgery
s.10 Computer-related extortion and fraud	Article 8 - Computer related Fraud
s.11 Identity theft	
s.12 Theft of telecommunication services	
s.13 Disclosure during an investigation	
s.14 Failure to provide assistance	
s.15 General procedural powers	
s.16 Search and seizure	
s.17 Admissibility of evidence	
s.18 Expedited preservation of stored computer data	Article 16 - Expedited Preservation of Stored Computer Data

s.19 Expedited preservation and partial disclosure of traffic data	Article 17 - Expedited Preservation and Partial Disclosure of Traffic Data
s.20 Production order	Article 18 - Production Order
s.21 Search and seizure of stored computer data	Article 19 - Search and Seizure of Stored Computer Data
s.22 Real-time collection of traffic data	Article 20 - Real time collection of traffic data
s.23 Interception of content data	Article 21 - Interception of content data
s.24 General principles relating to international cooperation	Article 25 - General principles relating to mutual assistance
s.25 Extradition	
s.26 Spontaneous information	Article 26 - Spontaneous Information
s.27 Confidentiality and limitation on use	Article 28 - Confidentiality and limitation on use
s.28 Expedited preservation of stored computer data	Article 29 - Expedited preservation of stored computer data
s.29 Expedited disclosure of preserved traffic data	Article 30 - Expedited disclosure of preserved traffic data
s.30 Mutual assistance regarding access to stored computer data	Article 31 - Mutual assistance regarding access of stored computer data
s.31 Transborder access to stored computer data with consent or where publicly available	Article 32 - Transborder access to stored computer data with consent or where publicly available
s.32 Mutual assistance regarding the real-time collection of traffic data	Article 33 - Mutual assistance regarding the real-time collection of traffic data
s.33 Mutual assistance regarding the interception of content data	Article 34 - Mutual assistance regarding the interception of content data
s.34 24/7 Network	Article 35 24/7 Network
s.35 35. Regulations	
s.36 Consequential amendments	



Datec (Fiji) PTE Ltd

Head Office:  
Level 1, Garden City Complex  
Grantham Rd, Raiwai  
Suva, Fiji Islands  
Tel: +679-331 4411  
Fax +679-330 0162

Branch Office:  
1<sup>st</sup> Floor Sunlight Building,  
Deo Street, Namaka  
Nadi, Fiji Islands  
Tel: +679-672 0181  
Fax: +679-672 0194

---

**Ref: Parl 6/16**

**Date: 3<sup>rd</sup> October 2022**

Parliament of the Republic of Fiji  
Standing Committee in Foreign Affairs and Defence  
Parliament Complex  
Constitution Avenue  
Suva

**RE: Request Face to Face Submission on the Convention on**

**Cybercrime** Dear Committee,

The world is witnessing an exponential increase in Cybercrimes. One of the latest examples being “OPTUS massive Data Breach” in the month of September that had exposed about 40% of the populations Personal Data.

Proactive measures are necessary to control or reduce such breaches by implementing required governance, framework and processes aligned with criminal justice, judiciary, prosecution, and law enforcement.

To prevent Cybercrime – Companies, Authorities and individuals need to implement Cyber Hygiene to keep sensitive data secure and protect it from theft or attacks. It is necessary to defend against sophisticated threats and collaborate to build more secure and resilient infrastructure in the Country.

To maintain an evolving and proactive secured posture all the stakeholders should implement sound practices, framework and solution to prevent cyber breaches.

Not only cyber-Security practices but also CERT is necessary in the Country.

Hence, as an ICT Solutions Provider in Fiji and the South Pacific, we recommend a National Legislation to deter and combat Cyber Crimes. However, as becoming a member of the Convention concerns National and International co-operation, exchange, compliance and concerns nations security, a

decision on joining the Convention should be made subject to approval from the Ministry of Foreign Affairs, Information and Communications, Defence, Financial Intelligence Unit and Human Rights.

Vinaka.



Pramendra Pal

**Pre-Sales & Sales Bid Manager**

**Datec Fiji PTE Limited**

Level 1 Garden City Complex, Gratham Road, Raiwai, PO Box 12577, Suva, Fiji | [www.datec.com.fj](http://www.datec.com.fj)

Phone: **+679 3314 411 Extn : 207** | Fax: +679 3300 162 | Helpdesk: + 679 3304 239 | Mobile: + 679 999 5717 | Email: [pramendrap@datec.com.fj](mailto:pramendrap@datec.com.fj) |

 <b>datec</b>	Contact us for more information:		
	<b>DATEC (FIJI) PTE LIMITED</b> P O Box 12577, Suva. <a href="http://www.datec.com.fj">www.datec.com.fj</a> <a href="mailto:info@datec.com.fj">info@datec.com.fj</a>	<b>HEAD OFFICE</b> Level 1, Garden City Complex Gratham Road, Raiwai P. +679 <b>331 4411</b> F. +679 <b>330 0162</b>	<b>NADI OFFICE</b> 1st Floor, Sunlight Building Deo Street, Namaka P. +679 <b>672 0181</b> F. +679 <b>672 0194</b>
<a href="https://facebook.com/Datecfiji">facebook.com/Datecfiji</a>			



## FIJI POLICE SUBMISSION

### Convention on Cybercrime

*The Hon. Chair of the Parliament Standing Committee on Foreign Affairs & Defence, Hon. Alexander O'Connor, Committee representatives, ladies and gentlemen. My task this morning is to present the Fiji Police Force's contribution towards the Committee's Review of the Convention on Cybercrime, otherwise known as the Budapest Convention.*

- 1.0 First and foremost, the Fiji Police Force (FPF) fully supports the Fijian Government in the process of reviewing the Cybercrime Convention. This is critical to our relations with other countries, in terms of development aid, foreign direct investment and multi-lateral partnerships. The scope of aspiring to have full rights to access the implementation of the convention shall be fully realised should Fiji accede to the convention. This will also bolster Fiji's commitment towards cybercrime in Fiji and the region in terms of the effective execution of duties as law enforcement officers.
- 2.0 In addition, the convention is a vital tool for the protection of all Fijians as the legal framework surrounding cybercrime shall be strengthened and the rights of all citizens shall be upheld.

- 3.0 As a law enforcement agency, the FPF is sanctioned under the Government's National Development Plan to protect all Fijians from environmental risks and natural disasters, transnational crimes (human and drug trafficking), food and nutrition security and public health risks and financial and cybercrime. The FPF therefore strives to enforce laws and legislation that falls under its mandate, i.e. the Cyber Crime Act of 2021.
- 4.0 At the outset, the Cybercrime Act of 2021, comprehensively addresses cybercrime by prescribing computer-related and content-related offences, providing procedural requirements including the collection of electronic evidence and international cooperation, providing the remedies in relation to cybercrime and for related matters. Therefore, the ratification of the convention will synchronise the *Cybercrime Act 2021* that was recently passed in parliament on 11 February 2021, as it mirrors the various sections of the Convention. Fiji also has the Online Safety Act 2018 for the promotion of online safety, deterrence of harmful electronic communication and for related matters.
- 5.0 The growing threat of the global cybercrime to Fiji and the Pacific is a concern. There is an urgent need for the FPF to have full digital access to and be compliant with other law enforcement jurisdiction for international cooperation on the investigation, enforcement and prosecution of cybercrime. In terms of data security, the FPF has a secure IT system that has been

safeguarding our digital information from corruption, theft, or unauthorized access.

6.0 The recognition to be fully equipped with investigative enablers such as the Budapest Convention is most needed now than ever. There have been difficulties faced whilst trying to locate the suspect if a case is reported through social media and it is even worse when a suspect is based in another country. Strengthening such mechanisms is therefore necessary to ensure that perpetrators are located and dealt with. Further to this, a cybercrime is registered as Police Enquiry Paper (PEP) as soon as the report is received either at the station level or referral CID HQ and is only converted to Registered Case when a perpetrator is arrested and charged. There have also been some PEP cases pending since 2015. Some PEP cases have been filed as complainants do not want any police action.

7.0 In terms of cybercrime statistics, a total of 45 cases was registered between the years 2016 to 2021. This includes the following cyber relate offences:

- a) Authorized Modification of Data held in a Computer
- b) Serious Computer Offences
- c) Unauthorized Modification of Data to Cause Impairment
- d) Unauthorized Modification of Restricted Data
- e) Causing harm by posting electronic communication, and
- f) Posting an intimate visual recording.

- 8.0 In addition, the FPF registered a total of 3 females and 8 male victims, and one female and 6 male offenders from 2016 to 2021. The statistics may not be that significant since Fijian people are not so forthcoming in reporting cyber related cases. This may be due to increased access to technology whereby criminals need not be physically present at the scene to commit a crime. Also, cases have not been reported due to the social stigma faced by victims who report such cases. The Fiji Police Force therefore shall continue to provide data on cybercrime to the FPF's relevant stakeholders, strive for a more inclusive approach to enhance our reporting structure and provide gender disaggregated data on cybercrime for the benefit of our relevant working partners as we effectively deal and respond to cyber related cases.
- 9.0 The FPF continues to venture into engaging with external stakeholders through its international relations portfolio to explore avenues in advancing Fiji's response against cybercrime. Hence, the continued commitment on capacity building to effectively respond to cybercrime. Police officers have been attending training locally and internationally in collaboration with our partners such as the Australian Federal Police and Cyber Safety Pacifica. This will ensure that the FPF is well versed with cybercrime and the laws surrounding it. Knowledge on technology and its evolving apparatuses needs to be enhanced since the criminal environment is changing and computer hackers and genius operates in the border-less realm of cyberspace. Currently, no proper technological equipment is available such as

phone extraction machines that can retrieve messages and calls. However, the FPF is working on securing a phone extraction machine to address cybercrime issues. The FPF has to continue to forge ahead to be on par with the global digital system.

10.0 Several parties are joining hands in realising the national intent of building a safer Fiji.

The FPF have been capitalising on inter-agency machinery to further reinforce the existing legal frameworks under the Whole of Government (WoG) and whole of population approach in creating awareness on cybercrime to schools, villages and communities. However, more concerted efforts shall be manifested on awareness should Fiji ratify the Cybercrime Convention.

11.0 Furthermore, the FPF is appreciative of the collaborative efforts by regional and international counterparts in solving some challenging cases of cybercrime that emanated with drug busts in Fiji. This convention therefore, shall allow the FPF to contact and allow easy access to any member state that is party to this Convention through their focal points for data, information and evidence.

12.0 The Convention shall also safeguard Fijian citizens from unnecessary exorbitant monetary loss, bankruptcy and economic leakage, online defamation of character, suicide or any action that may be detrimental to Fijians.

## **Ratification**

13.0 The FPF fully supports the ratification of the Cybercrime Convention as this will endorse Fiji's obligations towards its commitment towards the international community and global safety and security emanating from the ever increasing interconnectivity to the world wide labyrinth of communications, information and telecommunications through various traditional and emerging means.

<<<< *Ends* >>>>

## Cybercrime cases [2016-2021]

Computer-related offences	2016	2017	2018	2019	2020	2021
Authorized Modification of Data held in a Computer	5					
Serious Computer Offences		3				
Unauthorized Modification of Data to Cause Impairment			1			
Unauthorized Modification of Restricted Data				32		
Causing harm by posting electronic communication						3
Posting an intimate visual recording						1

*Source: Fiji Police Crime Statistics Unit, 2022*

The table above shows the number of cyber-related cases over a 6-year reporting period. These are all detected cases where all offenders were arrested and charged.

## GENDER ANALYSIS

Type	Gender	2016	2017	2018	2019	2020	2021
Victim	Female	1		1			1
	Male	4	1		1		2
Offender	Female				1		
	Male	1	1	1			3

*Source: Fiji Police Crime Statistics Unit, 2022*

### Note

In 2016 – there was a case involving 5 victims and 1 offender

In 2017 – there was a case with 3 counts

In 2019- there was a case with 32 counts

In 2021 – there was a case with 2 counts involving a female victim and male offender



## OFFICE OF THE DIRECTOR OF PUBLIC PROSECUTIONS

---

GUNU HOUSE, 25 GLADSTONE ROAD, SUVA, FIJI

PO BOX 2355, GOVERNMENT BUILDINGS, SUVA, FIJI

TEL NO: (679) 321-1250

FAX NO: (679) 330 - 2719

---

11<sup>th</sup> October 2022

The Hon. Alexander O'Connor  
Chairman, Standing Committee on Foreign Affairs and Defence  
Parliament Complex  
Constitution Avenue  
**SUVA**

Dear Sir,

**Re: ODPP Submission on the Budapest Convention on Cybercrime**

---

1. I refer to your correspondence to me dated 20<sup>th</sup> September 2022 requesting my appearance at present a submission on the Budapest Convention on Cybercrime (the "Convention") on Monday 26<sup>th</sup> September 2022.
2. I am grateful to the Standing Committee on Foreign Affairs and Defence (the Committee) for granting me additional time within which to make our submissions which are outlined below and for the opportunity to present them directly to the Committee today.

### **Background**

3. The Convention is currently being considered by the Committee for accession.
4. The Director of Public Prosecutions (the DPP) has been invited by the Committee to make submissions.
5. Under Fiji's legal framework, the Office of the Director of Public Prosecutions (the ODPP) is the main prosecutorial body responsible for undertaking any prosecutions under any law in Fiji.
6. Under the mutual legal assistance framework (Mutual Assistance in Criminal Matters Act 1997 (MACMA)) and the extradition framework (Extradition Act 2003), the DPP is given the authority to proceed to make relevant applications in the Courts.

### **Analysis of the Convention and Fiji's Existing Legislation**

7. The Convention makes it mandatory for State parties to criminalise offences as highlighted in Section 1 – Substantive Criminal law.
8. We note that the Cybercrime Act has been enacted but is not yet in force. The Cybercrime Act is the main legislation designed to ensure that Fiji will conform to its obligations under the Convention. If Fiji accedes to the Convention, other Acts will also require amendment.
9. The table below summarises the relevant details.

Convention	Law of Fiji	Comments
Article 2	Cybercrime Act 2021 (CYB) s 5 (1)	
Article 3	CYB s6	
Article 4	CYB s7	
Article 5	CYB s7	
Article 6	CYB s8	
Article 7	CYB s9	
Article 8	CYB s10	
Article 9	Juvenile Act s62A	The provision of the Juvenile Act is not as wide as the convention. In particular, it seems as if mere possession on a computer as required under Article 9(1) (e) is not criminalised.
Article 10	Copyright Act	
Article 11	Crimes Act s 44, 45	
Article 12	CYB penalty provisions have sanctions for body corporate.	
Article 14	CYB s15	
Article 16	CYB S13	
Article 17	CYB s19	
Article 18	CYB S20	
Article 19	CYB S21	
Article 20	CYB S22	
Article 21	CYB S23	

Article 22	Crimes Act s7	Fiji does not apply extra territorial jurisdiction on its nationals and the Convention does not make this mandatory.
------------	---------------	--

### **International Cooperation**

10. The Cybercrime Act 2021 makes some provisions for international cooperation in Part 6.

### **Extradition (Article 24)**

11. All the offences under the Cybercrime Act 2021 would be considered extraditable.
12. Fiji applies a dual criminality requirement for any extradition requests made to Fiji. With the exception of possessing child pornography which is not an offence in Fiji, the offences outlined in the Convention would all be considered extradition offences.
13. Fiji's extradition scheme allows for extradition from treaty countries, Pacific Island countries, and Commonwealth countries. Countries can also be declared Comity countries if they do not fall under these categories.
14. Under section 61 of the Extradition Act 2003, Fiji can choose to prosecute instead of extraditing.
15. The Convention does not place additional requirements on extradition as they are already outlined in the Extradition Act 2003.

### **Mutual Legal Assistance**

#### **Article 25**

16. MACMA already allows for an expedited means of sending requests.
17. We do not have dual criminality requirements for mutual legal assistance requests under the MACMA.

#### **Article 26**

18. With the exception of the Financial Intelligence Unit, none of Fiji's law enforcement agencies do spontaneous sharing of information, and the convention makes it discretionary.
19. Section 26 of the Cybercrime Act also makes the spontaneous sharing of information discretionary.

#### **Article 27**

20. Under MACMA, Fiji already designates a Central Authority for sending and answering requests.

21. The grounds for refusal of a request are already part of MACMA.
22. Confidential requirements apply to all requests under MACMA.
23. Under MACMA, all requests need to be directed through the Central Authority, that is, the Attorney-General, but under Article 27 (9) of the Convention there are provisions for sending requests directly to law enforcement agencies.
24. Given that the granting of MLA requests is an executive decision, it is our view that all requests should be directed through the Attorney-General's office and appropriate permissions obtained before proceeding. Any other way is in breach of s. 9 (4) of MACMA.

#### Articles 29 and 30

25. In relation to the preservation of stored computer data (Article 29) again there is a provision that the preservation can occur before the formal request is submitted.
26. Section 28 of the Cybercrime Act 2021 also allows for the preservation of data to occur before a formal request is sent.
27. Under section 13 of MACMA, however, the Attorney-General must authorise a law enforcement agency such as the Police to conduct a search and retrieve evidence which is by way of Magistrates' Court warrant.
28. There appears to be a conflict between the two Acts whereby the Cybercrime Act is replicating the obligations under the Convention but overriding the protections given under the MACMA.

#### Article 31

29. This is in line with MACMA that there needs to be a formal request to the Attorney-General.
30. Section 30 of the Cybercrime Act 2021 expands the MACMA provisions from sending the request to the Attorney-General to now sending it to the investigating authority.

#### Articles 32 and 33

31. This is in line with the MACMA that there needs to be a formal request to the Attorney-General. The Cybercrime Act 2021 is also in line with the MACMA.

#### Article 35

32. There is an obvious issue in relation to having a point of contact 24/7 because the ODPP which is intrinsically linked to criminal matters, mutual assistance and extradition does not have the ability to be available 24/7 to assist any contact point who may be nominated.

33. In order for the ODPP to support a 24/7 contact system, the ODPP would require greater resources than are currently budgeted.

#### **Proposed Amendments to the Cybercrime Act**

34. The Cybercrime Act should be amended to ensure that all requests go through the Attorney-General as they currently do under the MACMA.
35. In our view, it is important that the Attorney-General, as the Central Authority under the MACMA, be maintained as the first point of contact under the Convention and under the Cybercrime Act so as to act as a filter and protection against unsanctioned or fraudulent requests and to allow the Fijian government to balance its foreign policies with those of the request from a requesting party.
36. The ability of foreign requesting parties to circumvent Fiji's competent authority and go directly to a law enforcement agency such as the police potentially risks (i) allowing a request from a malevolent source such as a criminal organisation to obtain confidential information and (ii) facilitating a request contrary to Fiji's foreign policy, for example, if the request comes from a party that Fiji does not have diplomatic relations with or has a policy of limited diplomatic relations.
37. Due to Fiji's small size, there is little practical delay in having requests go through the Attorney-General as has been seen in recent mutual legal assistance requests, such as the United States' request concerning seizure of the Amadea superyacht.
38. To date, all mutual legal assistance requests have been dealt with expeditiously. There is no reason this should not continue.

#### **Proposed Amendments to the Juveniles Act**

39. We note that the Cybercrime Act has amended the Juveniles Act by section 62A however whilst the amendment defines pornographic activity in broad terms as it relates to children it does not appear to criminalise the simple possession of child pornography on a computer.
40. The possession of child pornography on a computer system would need to be included in the Juveniles Act or possibly as a separate offence under the Crimes Act in order to conform to Article 9 (1) (e) of the Convention.
41. Currently the simple act of possession of child pornography is not a criminal offence in Fiji.

## **CONCLUSION**

42. The Convention represents a progressive move towards the facilitation of greater international co-operation in dealing with cybercrime.
43. It is our submission that Fiji should accede to the Convention but with reservations to Article 27 (9) (a) – (e) and Article 31 as is allowed for under the Convention.
44. It is also our submission that the Cybercrime Act and the Juveniles Act require further amendments:
  - i. the Cybercrime Act should be amended to ensure and that all requests from requesting countries go through the Attorney-General as they currently do under the MACMA;
  - ii. The Juveniles Act should be amended to criminalise the simple act of possession of child pornography.
40. Appropriate budgetary resources are allocated to the ODPP and other agencies in order to prepare for Fiji's accession to the Convention particularly with respect to the 24/7 network establishment.

Thank you.

Yours faithfully,



Christopher T. Pryde

**Director of Public Prosecutions**



## **FIJI WOMEN'S CRISIS CENTRE SUBMISSION:**

## **CONVENTION ON CYBERCRIME (BUDAPEST CONVENTION)**

# Acronyms

<b>Budapest Convention</b>	<b>Convention on Cybercrime</b>
<b>FWCC</b>	<b>Fiji women's Crisis Centre</b>
<b>ICT</b>	<b>Information Communications Technology</b>
<b>OGBV</b>	<b>Online Gender Based Violence</b>

## 1. BRIEF ON FIJI WOMEN'S CRISIS CENTRE

The Fiji Women's Crisis Centre (**FWCC**) is a human rights organisation, based on the principles of human rights, democracy and the rule of law which has been in existence for over 38 years.

The goal of FWCC is to eliminate all forms of violence, in all spheres of life, against women in Fiji and the Pacific. FWCC implements this vision through an integrated and comprehensive program designed to prevent and respond to violence, by reducing individual and institutional tolerance of violence against women, and increasing available and appropriate services for survivors.

FWCC addresses the problem of violence against women using a human rights and development framework. This focus on human rights includes a feminist analysis of the problem and permeates all aspects of FWCC's work, recognising that the root causes of violence against women are unequal gender power relations, imbedded in Patriarchy.

## 2. INTRODUCTION

Violence against women is a pandemic that is globally recognised as a political, social and health problem. It is a grave violation of human rights. In Fiji, 64% of Fijian women who have been in an intimate partner relationship experienced physical or sexual violence or both by their husband or intimate partner in their lifetime.<sup>5</sup> This is almost double the global average. While efforts from Non-Government Organisations (NGO), State and other stakeholders have more than doubled in the recent past, it is evident that it still remains a crisis. One that is exacerbated by natural disasters, political upheavals and pandemics.

The exacerbation of this crisis has now translated onto the virtual platform. Cybercrime is quick to occur and difficult to prosecute. Network intrusions and "hacks" can take place in a matter of seconds with complete anonymity. And those that do leave criminal trails do so through a maze of computer infrastructure,

---

<sup>5</sup> Fiji Womens Crisis Centre, National Research on Women's Health and Life Experiences in Fiji (2010/2011): A survey exploring the prevalence , incidence and attitudes to intimate partner violence in Fiji, *Somebody's Life Everybody's Business*, 2013, p. 146

Information and communication technologies (ICT) have transformed societies worldwide and is now a lifeline for many, especially during the COVID-19 restrictions/isolations. However, ICT has also made societies highly vulnerable to security risks such as cybercrime.

Appropriate safeguards and a unified effort nationally and internationally can assist in tackling cyber related offences.

The Convention on Cybercrime (Budapest Convention) can provide the framework that Fiji can use to strengthen its Cybercrime Legislations and policies. The treaty's objectives are three-fold:

- 1) harmonizing national laws related to cyber-related crime;
- 2) supporting the investigation of these crimes; and
- 3) increasing international cooperation in the fight against cybercrime<sup>6</sup>

We welcome this opportunity to assist this Standing Committee in reviewing the Budapest Convention and we commend the State for considering becoming a State party to this Convention.

This paper will review and discuss whether Fiji should become a State party to the Cybercrime Convention also known as the Budapest Convention.

### 3. CHALLENGES OF THE CONVENTION

#### 3.1 Procedural Safeguards

While it is sometimes referred to as the “gold standard” because it is the most comprehensive multilateral cybercrime treaty, the Budapest convention has been critiqued for not having stronger safeguards for human rights.

While the Convention lacks privacy and civil liberties protections, the procedural provisions are vague and ambiguous. Consequently, this gives a lot of room for States to empower their law enforcement agencies to carry out acts that can encroach on the preservation of human rights and democracy.

For instance, the surveillance powers that this Convention would hand to enforcement agencies are not balanced out by meaningful privacy or civil

---

<sup>6</sup> Convention on Cybercrime, Council of Europe, <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>

liberties restraints. Unlike other international law enforcement agreements (including the Interpol, Europol and Schengen agreements), this Convention does not include specific provisions to protect citizens' privacy. In fact, the word "privacy" doesn't appear once in any of the articles.<sup>7</sup>

Another example is the weak protection that the Convention has when dealing with political activities. The term "*political offences*" is not defined and this ambiguity can be used to silence citizens and human rights defenders. This poses a real danger to the spirit of democracy, human rights and rule of law for our nation. Definitions are fundamental; for the law uses definitions to separate issues of fact from issues of law.

Under the Convention, Fiji's assistance could be authorized in many cases solely by law enforcement which can be without any judicial approval or oversight. And since the Convention doesn't even have a reporting requirement (requiring instances of cooperation with other countries on foreign crimes to be made public), law enforcement decisions on this sensitive issue may never be subjected to civilian check or oversight. The threshold for the use of this powers by law enforcement is not properly defined within the Convention and this poses a danger to human rights, rule of law, and democracy as this power can easily be abused.

Without proper safeguards in place, this Convention will empower law enforcements to carry out improper surveillance and unnecessary intrusions into the lives of our citizens under the pretext of cybercrime. Should Fiji decide to become a State Party to this Convention, then we urge that Fiji ensures that human rights, democracy and the rule of law be placed at the centre of Convention to avoid a one-sided application and enforcement in the future. In addition, having proper procedural safeguards in place will neutralise the threat to human rights and civil liberties.

### 3.2 Gender

While the Convention is comprehensive and provides a coherent framework addressing cybercrime offences, the Convention does not take into account Gender. Gender shapes and influences online behaviour and it also affects access to justice for survivors/victims of Online Gender Based Violence (OGBV) such as cyberstalking, revenge porn, sextortion, gender-based violence hate speech, etc. Online gender dynamics strengthens and amplifies gender inequalities that already exists in the offline world. Cybercrime also impacts

---

<sup>7</sup> There is one platitude about privacy in the preamble.

people based on their gender identity; however, it is not gender neutral and neither should our response to it be.

If Fiji decides to accede or ratify this Convention, then we urge that Fiji integrates a gender perspective in the implementation and enforcement of the Convention in our domestic context. This will help us to create effective laws, policies and procedures to efficiently prevent and combat cybercrime.

We also urge that Fiji also considers other conventions which offer more protection to women and girls such as the Convention on Preventing and Combatting Violence Against Women and Domestic Violence (Istanbul Convention), to work hand in hand with the Budapest Convention to ensure better protection of our women and girls and the recognition of online GBV being a violation of a woman's human right.

#### **4. ADVANTAGES OF THE CONVENTION**

Online Gender based Violence (OGBV) takes many forms and is often intersectional in nature, meaning that women from diverse and vulnerable communities are disproportionately (and often more severely) impacted. Globally, rates of OGBV are increasing, with spikes being experienced during COVID-19 lockdowns/isolation. Fiji's experience was no different; the Fiji women's Crisis Centre Statistic showed a dramatic increase in the number survivors between 2018 To 2021; even more so during COVID-19 lockdowns/isolation.<sup>8</sup> It also showed that the survivors were predominately women.

Women are disproportionately targeted to experience every form of online abuse. OGBV thrives where gender inequality is already well-entrenched, is rooted in misogyny, and is designed to control and silence women online. Online abuse of women and girls is more violent, sexualised and is focused on appearance than online abuse experienced by men. The United Nations reports that 73% of women online have been exposed to online abuse and that women are 27 times more likely to experience online harassment than men. The online abuse that younger women (ages 18-24) experience often includes more dangerous forms of stalking and violence<sup>9</sup>.

---

<sup>8</sup> Annexure 1

<sup>9</sup> *Final report of the Broadband Commission Working Group on Gender, September 2015*  
<https://en.unesco.org/sites/default/files/highlightdocumentenglish.pdf>

Unfortunately, enforcement agencies tend to minimise the severity of online abuse, despite its very real physical and psychological consequences. Most survivors of OGBV just want the violence to stop, while others may want the person to be charged and prosecuted. Some survivors may want to increase the security and privacy of their technology to prevent or minimise the abusive person's contact. All Survivors want their perpetrators to **STOP** the harassment online and any harmful post to be brought down as soon as possible.

In the last quarter, FWCC has noted a trend where harmful posts are taking longer to be removed from the internet. Reasons have ranged from law enforcers lacking the jurisdiction, to law enforcers being unaware of the law, to the expertise or resources needed to bring posts down not being available.

The Budapest Convention's primary focus is on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security.<sup>10</sup> It provides a framework that permits hundreds of practitioners from State Parties to share their experience and create relationships that facilitate cooperation in specific cases, including in emergency situations, beyond the specific provisions foreseen in this Convention. The Convention could help build the capacity of countries with less experience in tackling cybercrime and provide the basis for technical assistance. This means that Fiji will have a network of experts to lean on in order to build capacity and provide expertise and resources when responding to crimes committed online. This is especially important for survivors of OGBV who need transparent and swift responses as well as effective remedies.

## RECOMMENDATIONS

1. While Fiji Does have a Cyber Crimes Act 2021 already in place, we do recommend that Fiji accede to the Budapest Convention.
2. While acceding to the Convention, the challenges noted above needs to be considered. It's high time we started talking about the balance we want between our security and our privacy in the digital age. Investing in rights-

---

<sup>10</sup> IBID 2

protecting alternatives is the right way to go.

3. While we commend Fiji for considering becoming a State party to the Budapest Convention, it is important to note that women and girls need far more than what the Convention can present. Therefore, it might be wise for Fiji to also consider other conventions which offer more protection to women and girls such as the Istanbul Convention, to work hand in hand with the Budapest Convention to ensure better protection of our women and girls and the recognition of online GBV being a violation of a woman's human right.

## ANNEXURES

### BIBLIOGRAPHY

#### BOOKS:

1. Fiji Women's Crisis Centre, National Research on Women's Health and Life Experiences in Fiji (2010/2011): A survey exploring the prevalence, incidence and attitudes to intimate partner violence in Fiji, *Somebody's Life Everybody's Business*, 2013, p. 8, 146

#### ONLINE RESOURCES:

1. Convention on Cybercrime, Council of Europe, <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>
2. *Final report of the Broadband Commission Working Group on Gender*, September 2015  
<https://en.unesco.org/sites/default/files/highlightdocumentenglish.pdf>
3. THE ISTANBUL CONVENTION <https://rm.coe.int/168008482e>

**Cybercrime: An escalating threat to modern business and customers**  
12 October 2022

**Cybersecurity Crime**

WE ARE **W GROUP**

1

**Cybercrime & Cybersecurity**  
**Cybercrime & Accelerating Threats**

**Cybercrime**  
The term used to describe:

- crimes directed at computers or other information communications technologies (ICTs) – computer intrusions or denial of service attacks
- crimes where computers or ICTs are an integral part of an offence (such as online fraud)

**The accelerating threats Westpac sees and key industry examples**

**Nation-state espionage**

As an organisation continuously or under false pretences that have cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party

**Insider threat**

The threat that an insider will use his or her authorised access, willingly or unwittingly, to do harm to the organisation's mission, resources, personnel, facilities, information, equipment, networks, or systems

**Issue-motivated hacktivism**

The act of invading a computer system or network for a socially or politically motivated reason

**3 threat volumes**  
in the last 12 months, responded to 372 phishing sites impersonating Westpac Group brands.

WE ARE **W GROUP**

2

**Threat intelligence**

**Externally-perceived increase in threat**

**Trends in significant incidents globally**

- Targeted ransomware**  
This year has seen a significant increase in criminal groups using advanced techniques for extortion, containing business disruption and reputational risk.  
Example: Colonial Pipeline, JBS Foods
- Espionage & critical infrastructure attacks**  
Nation state attacks on critical infrastructure or sensitive data, increasingly affect private sector.  
Example: Solarwinds compromise affecting 160,000 US Gov.
- Collateral Damage from 3rd party incidents**  
Increased volumes of successful attacks on companies seen, unauthorised data access and business disruption impacts flow through supply chains. Example: Thompson, Landfill, Office.

WE ARE **W GROUP**

3

**Cybercrime & Cybersecurity**  
**Cyber Controls**

Westpac has a layered set of cybersecurity controls in place, as part of a defence-in-depth strategy.

**Cyber smart, cyber safe**

WE ARE **W GROUP**

4

**Cybersecurity capabilities to defend threats**  
Capabilities are deployed in layers to prevent, contain & detect threats

WE ARE **W GROUP**

5

**Cybercrime & Cybersecurity**  
**Customers & Community**

**How we help our customers**

- Educational materials
- Additional outreach
- Targeted awareness campaigns
- Phishing and malware protection

**How we contribute to the community**

- The following programs are established in Australia and soon to launch in Fiji
- Cyber Resilience Outreach Clinics
- Cyber Steps Program
- Participation in information sharing communities

**How we respond & manage cyber threats**

- Cyber Response Playbook

WE ARE **W GROUP**

6

**Improving threat intelligence collaboration**  
Broad collaboration helps inform our strategy & tactics

<p><b>Australian Industry (New Zealand)</b></p> <ul style="list-style-type: none"> <li>Isotank Forum – Cybercrime</li> <li>Isotank Forum – Security Testing</li> <li>Isotank Forum – Application Security</li> <li>ISG/CSSO Meetings</li> <li>CSSO Calls</li> </ul>	<p><b>MACQUARIE</b></p> <p><b>SUNCORP</b></p> <p><b>CISO LENS</b></p>	<p><b>International Industry (New Zealand)</b></p> <ul style="list-style-type: none"> <li>Financial Services Information Sharing and Analysis Center (FS-ISAC)</li> <li>Information Security Forum (ISF)</li> <li>New Zealand Internet Task Force</li> </ul>
<p><b>Australian Government &amp; Units</b></p> <ul style="list-style-type: none"> <li>ASD/ACSC Joint Cyber Security Centre and National Information Exchange</li> <li>CPA Cyber and Infrastructure Security Centre &amp; Trusted Information Sharing Network (TISN)</li> <li>ASIO</li> <li>Law Enforcement Agencies (LEAs) across state and federal police</li> </ul>	<p><b>ACSC</b></p> <p><b>AFF</b></p>	<p><b>International Government, Regulators and Units</b></p> <ul style="list-style-type: none"> <li>New Zealand Financial Services Information Exchange</li> <li>US Federal Bureau of Investigation (FBI), Secret Service</li> <li>UK National Cyber Security Centre (NCSC)</li> <li>Ministry of Security (MOS)</li> <li>Hong Kong Monetary Authority (HKMA)</li> </ul>

WE ARE **W GROUP**

7

**Cybercrime & Cybersecurity**  
**Questions**

WE ARE **W GROUP**

8



**FIJI REVENUE AND  
CUSTOMS SERVICE**

*Presentation to:*

**Parliament Standing Committee-Foreign Affairs and  
Defense committee on Convention on Cybercrime  
(Budapest Convention)**

**Name of Presenter:** Fiji Revenue and Customs Service (FRCS)

**Date:** 17 October, 2022

## OVERVIEW OF PRESENTATION

- FUNCTIONS OF FRCS [TAX AND CUSTOMS]
- CONFIDENTIAL INFORMATION AND SENSITIVE DATA
- REVIEW OF CYBERCRIME CONVENTION AND APPLICABILITY TO FRCS
- CHALLENGES
- WAY FORWARD
- CONCLUSION



**FIJI REVENUE AND  
CUSTOMS SERVICE**

## FUNCTIONS OF FRCS [TAX AND CUSTOMS]

The functions of FRCS is captured under Section 22 of the FRCS Act of 1998 which is as follows:-

- act as Agent of the State in providing services and administering and enforcing customs and tax laws;
- disburse loans or funds on behalf of the state;
- exercise all functions and perform all duties necessary for the collection and recovery of tax or customs duties;
- advise the State on matters relating to taxation and customs and excise;
- represent the State internationally in respect of matters relating to taxation, customs, and excise; and
- perform other such functions as the Minister may assign to the Service



FIJI REVENUE AND  
CUSTOMS SERVICE

## CONFIDENTIAL INFORMATION AND SENSITIVE DATA

- FRCS has a duty under Section 52 of the FRCS Act of 1998 to protect any confidential information and documents received from Taxpayers, Travellers or Traders whilst in the performance of our duties.
- Confidential information and or sensitive data that is received through its physical or electronic means are as follows:-
  - a) Personal information such as date of birth, their residential address, their bank details, passport, information of their personal assets, etc;
  - b) Company financials (Profit and Loss, Shareholding Structure, etc);
  - c) Importation or exportation data (SAD Entry, Bill of Lading, Invoices, etc)
  - d) Data on foreign Companies, entities, etc; and
  - e) Any other data acquired for the purpose of administration of Customs and Tax and Excise Laws.



FIJI REVENUE AND  
CUSTOMS SERVICE

## CONFIDENTIAL AND SENSITIVE DATA

- This confidential information or sensitive data is obtained through;
  - a) Lodgment of returns (Income Tax ,Value Added Tax, etc) for tax purposes;
  - b) Lodgement of SAD Entry (IM-4, IM-7, etc) for Customs purposes;
  - c) Information obtained through Administrative notice under Section 36 of the Tax Administration Act of 2009;
  - d) Seizures under Section 35 of the Tax Administration Act and under Section 129 of the Customs Act of 1986;
  - e) Information obtain through exchange by way of Double Taxation Agreements (DTA) and other information obtained through MOU's with other enforcement agencies; and
  - f) Voluntarily provided by the Taxpayer, Traveler or Trader.
- There is a need to ensure that legislative and other measures are in place to ensure that such confidential information is protected.



FIJI REVENUE AND  
CUSTOMS SERVICE

## REVIEW OF CYBERCRIME CONVENTION AND APPLICABILITY TO FRCS

- **Article 4 and 5-** There is no specific provision in the tax and customs laws where we can prosecute a Taxpayer for damaging, altering such electronic data or computer system. Recommend that we have such powers in our legislations.
- **Article 9-** provide legislative powers to Custom Officers to work closely with immigration and police officers in detaining any computer-data storage medium at the Border on reasonable grounds that such storage medium has child pornographic content;
- **Article 10-** Customs to be given legislative powers (ex-officio powers) to detain and destroy any goods that is in breach of any IPR laws identified at the Border that may have been procured by the Importer by means of a computer system;



FIJI REVENUE AND  
CUSTOMS SERVICE

## REVIEW OF CYBERCRIME CONVENTION AND APPLICABILITY TO FRCS

- **Article 19-** Section 35 and 36 of the Tax Administration Act of 2009 provides FRCS powers to furnish, seize or detain any electronic data and electronic data storage device for administering our tax law. No specific powers to detain electronic data in Section 129 of Customs Act of 1986 for customs purposes. Propose that such powers is also given to our Customs Act for electronic data and its data storage.
- **Chapter 3-** Section 52 of the FRCS Act maintains the importance of keeping any such electronic data relating to Taxpayers as confidential information. Chapter 3 and its related Articles discusses in length about international co-operation in terms of data sharing. This can be a challenge for our Organisation in terms of our secrecy provisions and how we are limited in terms of our Act when it comes to sharing any confidential information in any form.



FIJI REVENUE AND  
CUSTOMS SERVICE

## CHALLENGES

- Our current legislation only allows FRCS to obtain data only for exercising its powers in administering of tax and Customs and Excise laws only. It does not make specific sections that deal directly with cybercrime.
- Our Section 52 of the FRCS Act of 1998 limits FRCS capability to share information for the purpose of combating cyber crime in Fiji where certain conditions need to be met in order for such information to be shared to the relevant enforcement agency;
- In terms of monitoring and enforcing of Cybercrime, FRCS requires continuous enhancements of its technology to be able to detect or combat any latest cyber crime.



FIJI REVENUE AND  
CUSTOMS SERVICE

## WAY FORWARD

- Amending our existing tax and customs and Excise legislations to ensure that we are compliant to the requirements under the Cybercrime Convention.
- Provide more training opportunities for our staff in terms of identifying, monitoring and combating cybercrime.
- Continuous enhancement of our current technology to be able to identify, monitor and prevent cybercrime.
- More collaboration with other law enforcement agencies who are responsible for handling any cybercrime issues in Fiji.



## CONCLUSION

- FRCS Supports the Ratification of the Cybercrime Convention.





**FIJI REVENUE AND  
CUSTOMS SERVICE**

Questions?

THANK YOU

## **A Submission on the Ratification of the Convention on Cybercrime**

19 October 2022

The Convention on Cybercrime of the Council of Europe, known as the Budapest Convention, is an international convention on cybercrime. The convention provides guidelines for countries that are in the process of developing comprehensive national legislation against Cybercrime, and it also serves as a framework for international cooperation between the various States who have signed the treaty. It is the first international treaty seeking to address Computer crime and Internet crimes by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.

It was drawn up by the Council of Europe in Strasbourg with the active participation of observer states such as Canada, Japan and China. It is open for ratification to states that are not members of the Council of Europe.

The Convention on Cybercrime covers three major areas:

- It includes a list of crimes related to computers & matters related to it that each member country must have on its books. The treaty requires criminalization of offenses such as hacking, the production, sale or distribution of hacking tools, and an expansion of criminal liability for intellectual property violations (Articles 2-11).
- It requires each signatory to grant new powers of search and seizure to its law enforcement authorities. They include the power to force an Internet Service Provider (ISP) to preserve a citizen's internet usage records or other data, and the power to monitor a citizen's online activities in real time (Articles 16-22).
- It requires law enforcement in every participating country to assist police from other participating countries. (Articles 23-35).

### **Some Advantages to Adoption**

Becoming a signatory to this convention brings some advantages:

- The Convention provides a legal framework for international cooperation not only with respect to cybercrime (offences against and by means of computers) but with respect to any crime involving electronic evidence. This will be a good proven framework for Fiji to adopt.
- Parties share information and experience, assess implementation of the Convention, or interpret the Convention.
- Even if a State did not participate in the negotiation of the original treaty, a new party is able to participate in the negotiation of future instruments and the further evolution of the Convention. This is done by being part of the Cybercrime Convention Committee (T-CY).

BSP Financial Group Limited

 132 888 | +679 321 4300     [bula@bsp.com.fj](mailto:bula@bsp.com.fj)  
 Private Mail Bag, Suva, Fiji     [www.bsp.com.fj](http://www.bsp.com.fj)

- Access to technical assistance is to facilitate full implementation of the Convention and to enhance the ability to cooperate internationally. Also give the ability to the signatory to participate in the Cybercrime Programme Office (C-PROC) for worldwide capacity building.
- Parties to the Convention can sign and ratify the Second Additional Protocol to the Budapest Convention, which provides additional and expedited tools for enhanced cooperation and disclosure of electronic evidence, such as direct cooperation with service providers across borders or cooperation in emergency situations.
- Being party to this Convention will send a message to the world that Fiji cannot be a safe-haven for cybercriminals where they can hide without fear of consequence.

## Some Considerations

There are some consideration that needs to be made which could include;

- The convention focuses on cybercrime and does not cater for privacy and civil liberties with cyber-security in mind. The surveillance powers that this treaty potentially hands to authorities are unrestrained when a request or a cybercrime is suspected. The legislations adopted need to make sure civil liberties are guarded.
- The Convention covers a vast area as these days almost all high or medium level business is done through the means of computers. The Convention covers not only computer-related crimes, but any crime where the evidence could be in computerized form. Means need to be created to be able to access and scrutinised data in a timely matter.
- The Convention does not consider a "dual criminality" requirement meaning Fiji authorities would need to cooperate with investigations of activities that are illegal abroad but might be legal in Fiji. What would be the implications of such a request for Fiji?
- The Convention is silent of the issue of "fair use" in terms of intellectual property provisions which could significantly expand criminal liability for intellectual property.
- Costs to provision for the Convention could be a burden for the country and businesses operating in it. Due transition time is required for the adoption and implementation of this convention with clear communication strategies for individuals, communities and organisations.

## Global Cost of Cybercrime

Global cybercrime costs are on the rise, increasing 15 per cent year over year, according to a 2021 cyberwarfare report by *CyberSecurity Ventures*. By 2025, it is estimated that cybercrime will cost businesses worldwide US\$10.5 trillion annually.

With the global cost of cybercrime at US\$3 trillion in 2015, that's more than a threefold increase over a decade.

Cyber-attacks are a threat to businesses and industries of all sizes particularly the financial sector. With cybercrime rising by 600% during the pandemic, businesses are more vulnerable than ever to the financial and reputational repercussions of cyberattacks. This makes it even more important for businesses and organizations to make cybersecurity a priority and in turn for Fiji to join a global treaty that focuses on cybercrime.

The consequences of cybercrime extend beyond just financial repercussions. Businesses may also suffer from:

- Loss of data
- Theft of intellectual property
- Theft of financial or personal information
- Reputational harm
- Lost productivity

As cyber-attacks become more frequent and advanced, businesses and countries in general need to be prepared to respond to incidents.

For a bank like BSP the costs to safeguard our data and customers have grown significantly in the last 5 years, it has more than doubled, now constituting over 20% of our IT operational costs. Even so, without partnerships with other companies and service providers we will not be able to withstand a global onslaught of cybercriminals. By joining this Convention, Fiji will become part of a global endeavour to uphold common standards which will serve to safeguard the businesses and community in Fiji.

## **Recommendation**

As technology traverses our geographical borders in a more pervasive way than ever imagined, providing a never ending arena for those that want to defraud others, a concerted and unified standard approach through a treaty such as the Convention on Cybercrime will only help band nations together to provide ways and instruments to safeguard it businesses, institutions and its citizenry in general. It also is a framework that allows hundreds of practitioners from various parties to share experience and create relationships that facilitate cooperation in specific cases, including in emergency situations.

For a small island developing nation such as Fiji, with limited resources, having access to a global community with the same aim and shared information will be invaluable.

It is recommended that Fiji does ratify the Convention on Cybercrime but ensures that provisions to implement the requirements, if not already encapsulated in Cybercrime Act of 2021, are in place in a timely manner, and all stakeholders are given time and empowered to implement relevant instruments to proactively act on the requirements.

**Omid Saberi**  
**Chief Information Officer**  
**BSP Financial Services Limited**



MINISTRY OF DEFENCE, NATIONAL SECURITY AND POLICING

---

**WRITTEN SUBMISSION TO THE STANDING COMMITTEE ON  
FOREIGN AFFAIRS AND  
DEFENCE  
ON THE  
REVIEW OF THE CONVENTION ON CYBERCRIME  
(BUDAPEST CONVENTION)**

---

**MINISTRY OF DEFENCE, NATIONAL SECURITY AND POLICING SUBMISSION TO THE  
STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE ON THE REVIEW OF  
THE CONVENTION ON CYBERCRIME (BUDAPEST CONVENTION):**

The Honourable Committee Chair and Honourable Committee Members.

As Permanent Secretary for Defence, National Security and Policing, I submit herein a written submission on behalf of the Ministry of Defence, National Security and Policing which contains our comments on the Convention on Cybercrime or more commonly known as the Budapest Convention.

**Manasa Lesuma (Mr.)**

**Permanent Secretary for Defence, National Security and Policing**

## **1.0 Convention on Cybercrime**

Honourable Chair and Honourable Committee Members, as you all may be aware the Budapest Convention was opened for signature in Budapest, Hungary in November 2001 and has since shaped international norms and law as a means for criminal justice response to cybercrime.

For Fiji, the passing of the Cybercrime Act 2021 saw the alignment of our national legislation with the provisions and obligations as set out in the Budapest Convention. Technological advancement has exponentially grown, and this is evident in its multifaceted use across all sectors. Whilst this ensures that we seamlessly do business and general conduct of business processing, it also carries the opportunity for cyber related crime to increase.

This underscores the importance for Fiji as an upstanding international community partner to accede to the Budapest Convention.

## **2.0 Scope of Written Submission**

Honourable Chair and Honourable Committee Members, the Ministry's written submission will cover the following scope:

- **Summary of the Convention on Cybercrime (Budapest Convention)**
- **Fiji's Status;**
- **Why Fiji should accede to the Convention**
- **Benefits of acceding to the Convention from the perspective of the Ministry's functional role; and**
- **Recommendation**

## **3.0 Summary of the Convention on Cybercrime (Budapest Convention)**

Honourable Chair and Honourable Committee Members, the summary and fundamental pillars of the convention are as follows:

- **Standardizing Cybercrime Legislation**

The Budapest Convention provides a framework that outlines common standards in the cybercrimes environment. The convention comprises four (4) Chapters and forty-eight (48) articles which covers fundamental components of response to criminal activities in cyberspace. Articles thirty-six (36) to forty-eight contain the Final Provisions whilst article one (1) to article thirty-five (35) contains the main parts of the convention in the three (3) areas of:

- i. Criminalising activities against and by means of computers or any electronic device
- ii. Procedural law tools associated with the investigation of cybercrimes and acquisition of electronic evidence
- iii. International co-operation on cross-jurisdictional matters in cybercrime investigations and electronic evidence.

- **Capacity Building between law enforcement agencies**

Recently there is a propagated move towards capacity building to reinforce criminal justice capabilities on cybercrime.

- **Strengthening international cooperation amongst State Parties**

Furthermore, the convention also provides a framework in which acceding parties can be guided towards achieving a standardized and uniform legislation which encourages cooperation between state parties.

#### **4.0 Fiji's Status**

Honorable Chair and Honorable Committee Members, Fiji's Status concerning the Budapest Convention are as follows:

- **Fiji is yet to accede the Convention pursuant to Article 37. However Fiji has partially adopted the Convention**

Fiji has yet to accede the convention. However, Fiji has had several legislations which have adopted some of the provisions in the Budapest Convention.

These legislations are:

- i. Juvenile Amendment Act 1997
- ii. Posts and Telecommunications Decree 1989
- iii. Crimes Act of 2009 which contains ten (10) sections, under Computer Offence Section 336 to Section 346.
- iv. Cybercrime Act of 2021 Addresses Cybercrime by stipulating computer related and content related offences including procedural requirements, collection of electronic evidence and international co-operation.

The above four legislations have adopted Articles one (1) to Twenty-Two (22) and articles twenty-four (24) to thirty-five (35) of the convention.

## 5.0 Why Fiji should accede to the Convention?

Honorable Chair and Honorable Committee Members, highlighted below are our positions regarding the purposes justifying Fiji's accession to the Budapest Convention.

- **Relevance: Addresses the evolving nature of criminal activities within Cyberspace and covers main components of investigating Cybercrimes**

The Budapest Convention covers the main fundamental components of response to illegal activities by means of computers and electronic devices and the extension of these activities into cyberspace.

Fiji acceding to the Budapest Convention would entail the following benefits:

- i. It will appropriate the relevance of cybercrime laws to illegal cyber activities. The challenge of any nation state enacting cybercrime laws is to appraise the dynamic evolving nature of technology and the internet. Small island developing nations such as Fiji will have access to and benefit from the evolution of the convention, now and into the future, as a base platform for reviewing its cyber laws and regulations governing illegal activities in cyberspace.
- ii. **Enhance Fiji's ability to combat cybercrime** through capacity building and international co-operation, to better equip the investigative, prosecutorial and judicial functions.
- iii. **With international co-operation comes international standards.** Fiji's acceding would also entail compliance with international standards. Law Enforcement agencies' services in the areas of cybercrime investigations and prosecutions will need to align with international standards and best practices. This will strengthen and enhance the quality of services delivered by law enforcement and prosecutions.

## **6.0 Benefits of acceding to the Convention from the perspective of the Ministry's functional role**

Honorable Chair and Honorable Committee Members, highlighted below are the benefits of acceding to the Convention from the perspective of the Ministry of Defence, National Security and Policing's functional roles.

- **Enhances the proposed National Critical Infrastructure Cyber Incident Response and Recovery Policy Framework**

Fiji's acceding to the Budapest convention, would not only strengthen Fiji's retributive security mechanisms to threats in cyberspace, it would also greatly benefit cyber-related security thematic areas under the Ministry such as Critical Infrastructure. The Ministry of Defence is mandated in providing policy guidance on critical infrastructure security platforms to ensure a safe and secure Fiji for all.

Critical Infrastructure describes the physical or virtual assets or services that are essential for the functioning of society and the economy. Critical Infrastructure is so vital that its impairment or destruction would inflict a debilitating impact upon our physical or economic security or public health or safety. Any physical or virtual assets or services that is deemed as a critical infrastructure is of national importance.

Critical infrastructure is increasingly interrelated and interconnected, delivering efficiencies and economic benefits to operations. However, connectivity without proper safeguards creates vulnerabilities that can deliberately or inadvertently cause disruption that could result in cascading consequences across our economy, security and sovereignty.

The Ministry is currently working together with other government, public and private stakeholders in the development of a proposed National Critical Infrastructure cyber incident response and recovery framework to protect Fiji's critical infrastructure from all hazards, including the dynamic and potentially catastrophic cascading threats enabled by cyber-attacks.

This proposed framework will incorporate Critical Infrastructure Computer Emergency Response Teams (CI-CERT) and Critical Infrastructure Computer Security Incident Response Team (CI-CSIRT).

Designated information security experts will form the Critical Infrastructure Computer Emergency Response Team (CI-CERT) and is primarily responsible for the protection against, detection of and response to cybersecurity incidents within the critical infrastructure community.

The Critical Infrastructure Computer Security Incident Response Team, or CICSIRT, will consist of information security experts within each critical infrastructure organization whose main goal is to respond to critical infrastructure computer security incidents quickly and efficiently, thus regaining control and minimizing damage.

Parties to the Budapest convention would open opportunities to receive and share invaluable information of pervasive threats in cyberspace which would be best utilized by the CI-CERT and CSIRT Teams, for awareness and proactive protection initiatives within the critical infrastructure community.

- **Enhances the effectiveness of incident response capability of CI CERT and CSIRT with nation states and multinational agencies through International Cooperation**

Fiji's acceding to the convention would enhance the response components of the National Critical Infrastructure Cyber Incident Response and Recovery Framework, through international cooperation and collaborations with parties to the convention.

- **Ensures free flow of mutual requests and assistance through international co-operation and dual criminality**

From a response and retribution stance, cyber incidents within the critical infrastructure community requiring law enforcement response would be effectively and efficiently addressed through access to international co-operation mechanisms and capacity building.

## **7.0 Recommendation**

Honorable Chair and Honorable Committee Members, considering the security benefits, the Ministry recommends that Fiji **Accede and ratify the Convention on Cybercrime without reservation**

- **It is further recommended for more collaborative work and action between the Ministry of Communication and CI agencies on the Formulation of a Cyber Security legislation and Policy Framework which governs CI agencies**

## **Memorandum for the Standing Committee on Foreign Affairs and Defence of the Fijian Parliament on the Council of Europe Convention on Cybercrime**

### **Background.**

1. The Council of Europe Convention on Cybercrime, commonly referred to as the Budapest Convention, was agreed in 2001. It is the main agreement relating to tackling cybercrime internationally and requires Parties to the Convention to have appropriate laws and procedures to tackle cybercrime and to be able to provide assistance to other countries – for example the provision of evidence.
2. Fiji has been invited to accede to the Convention. The Standing Committee on Foreign Affairs and Defence has requested a memorandum which addresses the question as to whether Fiji should ratify the Convention. Some recommendations are set out in the final section of this paper.
3. The Convention has been ratified by 67 States, including all Council of Europe Members apart from Ireland<sup>11</sup>, as well as the United States, Australia, Canada and Japan.<sup>12</sup> Any State may accede to the Convention under the procedure set out in Article 37. Russia, which has recently departed the Council of Europe, opposes the Convention, stating that adoption would violate Russian sovereignty.
4. The preamble of the Budapest Convention describes its aims in the following way: A “common criminal policy aimed at the protection of society against cybercrime”. It intends “to deter action directed against the confidentiality, integrity, and availability of computer systems, networks and computer data as well as the misuse of such system, networks, and data by providing for the criminalization of such conduct.”
5. The Convention provides for (i) the criminalisation of conduct ranging from illegal access, data and systems interference to computer-related fraud and child pornography; (ii) procedural law tools to investigate cybercrime and secure electronic evidence in relation to any crime; and (iii) efficient international cooperation.
6. Substantive criminal offences under the Convention are set out in Articles 2-12 and include Illegal access (Art. 2); Illegal interception (Art. 3); Data interference (Art. 4) System interference (Art. 5); Misuse of devices (Art. 6); Computer-related forgery (Art. 7); Computer-related fraud (Art. 8); Child pornography (Art. 9); Intellectual property rights offences (Art. 10) Attempt, aiding, abetting (Art. 11); Corporate liability (Art.12).

---

<sup>11</sup> Ireland has signed the Convention. In January 2019, the Minister for Justice indicated that Ireland had not ratified the Convention on the basis that its domestic law was not compliant with its provisions, but that “the current Government Legislation Programme makes provision for the drafting of a new Cybercrime Bill to give effect to those remaining provisions of the Cybercrime Convention not already provided for in national law in order to enable ratification of the Budapest Convention.”

<sup>12</sup> [List of signatories to the Budapest Convention](#) (last accessed 21 October 2022)

7. The Convention requires States to ensure that the offences against Articles 2 to 12 are criminalised in their domestic law, and that their criminal justice authorities have relevant powers prescribed in their procedural law.
8. Article 15 of the Convention requires the Parties to uphold the protection of human rights and this includes rights arising out of obligations in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (commonly referred to as the European Convention on Human Rights) and the 1966 United Nations International Covenant on Civil and Political Rights, as well as other applicable international human rights instruments. The Council of Europe oversees the European Convention on Human Rights.
9. Under Article 27, Parties to the Convention may refuse a request for mutual assistance where the request concerns an offence which the requested Party considers a political offence, or an offence connected with a political offence, or it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public*, or other essential interests.
10. In July 2020, the Council of Europe published a report which aimed to highlight the benefits and impact of the Budapest Convention on Cybercrime in view of facilitating dialogue with States and stakeholders interested in cooperation on cybercrime.<sup>13</sup> In summary, the report concluded that:

“While any country may make use of the Convention as a guideline for domestic legislation, becoming a Party provides additional benefits:

  - it serves as a legal basis for international cooperation;
  - Parties contribute to the further evolution of the Convention through guidance notes or additional protocols;
  - membership in the Convention means membership in networks of practitioners, in particular the 24/7 Network of contact points established under this treaty;
  - Parties experience improved cooperation with the private sector;
  - Parties and States having requested accession to this treaty may become priority countries and hubs for capacity building.”<sup>14</sup>
11. The Convention has two additional Protocols. The first relates to the criminalisation of acts of a racist and xenophobic nature committed through computer systems, which was opened for signature in 2003.<sup>15</sup> The second Protocol was opened for signature in 2022 and relates to enhanced co-operation and disclosure of electronic evidence. Parties to the Convention can also become Parties to the two Protocols without the need for a further request for accession.

---

<sup>13</sup> <https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac> (last accessed 21 October 2022)

<sup>14</sup> Ibid.

<sup>15</sup> [List of signatories to the First Protocol](#) (last accessed 21 October 2022)

12. The Council of Europe indicates that where States become priority countries for capacity building programmes, technical assistance can be provided to facilitate full implementation of the Convention and to enhance their ability to co-operate internationally.<sup>16</sup>
13. Fiji was invited to accede to the Budapest Convention in December 2021.<sup>17</sup> The Council of Europe has indicated that the domestic legislation of Fiji “is now broadly in line with the Budapest Convention on Cybercrime.”<sup>18</sup> This assessment was recently supported by the Fiji Law Society, which indicated that many of the Articles of the Convention were reflected in the Cyber Crime Act 2021.

### **The UK position.**

14. The UK Government “strongly supported the Budapest Convention when it was signed in 2001”. It signed the Convention in November 2001 and ratified in May 2011. The UK Government argues that the Convention is “the most effective international instrument currently available for cooperation on cybercrime”.<sup>19</sup> It has consistently promoted the Convention.
15. In a recent Command Paper, issued in respect of the Second Additional Protocol to the Convention, the UK Government indicated that:

“The UK supports the Convention for a number of reasons. The Convention includes offences that are internationally understood, and which affect all societies. The Convention does not include offences in relation to freedom of expression, political views, national security, or terrorism, which do not have generally accepted definitions. The Convention is strongly rooted in human rights, ensuring that powers are used proportionately. Finally, the Convention is intended as an independent template for co-operation, and its design is clearly focused on supporting investigation and prosecutions. It does not cover regulation or internet standards, both of which are dealt with by other bodies.”<sup>20</sup>
16. The UK entered several reservations when it ratified the Budapest Convention. These included reservations:
  - (i) not to apply Article 9 (2) (b), which states that “child pornography” includes “a person appearing to be a minor engaged in sexually explicit conduct”, as this provision is incompatible with domestic law regarding indecent photographs of children.

---

<sup>16</sup> <https://rm.coe.int/cyber-buda-benefits-june2022-en-final/1680a6f93b> (last accessed 21 October 2022).

<sup>17</sup> [Fiji and Vanuatu invited to join the Budapest Convention on Cybercrime - News \(coe.int\)](#) (last accessed 21 October 2022).

<sup>18</sup> Ibid.

<sup>19</sup> [Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence \[MS No.9/2022\] - GOV.UK \(www.gov.uk\)](#) (last accessed 21 October 2022)

<sup>20</sup> Ibid.

- (ii) not to apply Article 29 where execution of the request for preservation requires the exercise of coercive powers and where dual criminality cannot be established.<sup>21</sup>

### Recent developments.

- 17. In 2022, the Council of Europe opened the Second Additional Protocol for signature. The Protocol builds on the Convention by providing a legal basis for enhanced co-operation between Parties to it, by requiring Parties to be able to permit competent authorities from another Party to request subscriber information and traffic data directly from the data owners; and more immediate co-operation in emergencies, underpinned by personal data protection safeguards.
- 18. An assessment of the key elements of the Protocol are set out in a Command Paper published by the UK Government in July 2022.<sup>22</sup> The UK intends to ratify the Protocol, but notes an issue under Article 10 (which deals with emergency mutual assistance). The UK is not yet fully compliant with this aspect of the Protocol, as it does not operate its central authorities responsible for responding to mutual legal assistance (MLA) requests on a 24/7 basis. Article 10(5), requires availability 24/7 in order to respond to MLA requests made in an emergency..
- 19. The UK Government has indicated that it will delay ratification of the Protocol until the UK is fully compliant with Article 10. The UK Government has also indicated that it will enter a reservation to Article 7 of the Protocol since the UK does not have a “clear legal framework to permit UK telecoms operators to respond to requests from overseas.”<sup>23</sup>
- 20. The Protocol was examined by the House of Lords International Agreements Committee at its meeting of 20 October 2022. The Committee reported the Second Protocol on 24 October 2022. It raised no objections to ratification, but noted that some NGOs and Members of the European Parliament have raised data and privacy concerns in relation to the Protocol. The Committee called on the Government to provide an assessment of the conditions and safeguards affecting the transfer of data under the Protocol and how compliance with the UK data protection regime would be ensured.<sup>24</sup>

### Recommendation.

- 21. **The Budapest Convention is a well respected Council of Europe agreement which is designed to prevent cybercrime. The Convention sets out a clear framework and any powers established under the Convention are designed to be used proportionately and subject to human rights norms.**

---

<sup>21</sup> A full list of the UK reservations can be found at: <https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=2&codePays=UK> (last accessed 21 October 2022)

<sup>22</sup> [Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence \[MS No.9/2022\] - GOV.UK \(www.gov.uk\)](#) (last accessed 21 October 2022).

<sup>23</sup> Ibid.

<sup>24</sup> [International Agreements Committee - Summary - Committees - UK Parliament](#) (last accessed 24 October 2022).

22. Notably, Parties to the Convention can refuse requests for mutual assistance where the request concerns an offence which the requested Party considers a political offence, or an offence connected with a political offence, or where it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public*, or other essential interests.
23. Acceding states are eligible to become priority countries for capacity building programmes.
24. The challenge for any Government considering whether to ratify the Convention is to ensure that its domestic law is compliant with the provisions of the Convention. The Convention requires State Parties to establish such legislative and other measures as may be necessary under its domestic law for a variety of criminal offences, as well as certain procedural provisions. The Council of Europe has indicated that the domestic law of Fiji is “broadly in line” with the Convention.
25. As can be seen from the situation in the United Kingdom, reservations may be required in circumstances where domestic law provisions do not currently comply with the terms of the Convention. It will no doubt be for the Ministry of Justice to highlight any provisions which have not been implemented in Fijian domestic legislation, or any other relevant incompatibilities.
26. Beyond these matters, I can see no reason which should preclude the Standing Committee on Foreign Affairs and Defence from recommending that Fiji should ratify the Budapest Convention.

**Alexander Horne**

Visiting Professor, Durham University

Counsel, Hackett & Dabbs LLP

Associate Member, Cornerstone Barristers

**24 October 2022**

# Budapest Convention Macro view

## Fiji – Micro view





13 April 2023

1
★

# Contributors

- **Semi Tukana** – Founder, Sole & Software Factory, Suva
- **Bob Adhar** – Founder, Randtronics, Sydney

2
★

# Macro view

- Fiji in process to ratify Budapest Convention on Cybercrime and has legislated CyberCrime Act 2021
- Constitution of the Republic of Fiji (2013) provides for a right to privacy but lacks specific personal data protection legislation
- GDPR set the standard, similar legislation now being passed and enforced worldwide
  - mandating the use of encryption to protect citizens data
- Effective encryption is now essential for protecting citizen's data and maintaining economic health


3
★

# Micro view

- Fiji should create its own privacy standard and enforce immediately – basically adopt Australian Data Privacy standard or GDPR or other similar standards.
- The standards should be mandatory to be implemented by all businesses and Government Departments in Fiji
- There should be fines (financial) and criminal implications if found negligent (that is, data is not protected).

4
★

# Security eco system 101 example




PCI Security Standards Council (Visa, Mastercard, Amex, JCB & Discover). Refer to standard for more detailed explanation.

**Cyber measures to protect data:**

- **Firewall** – maintain secure network by blocking unauthorized network traffic
- **Antivirus & malware** – maintain secure systems by targeting vulnerabilities
- **Access control** – restrict access to data by a need-to-know basis
- **Network Monitoring** – regularly monitor networks and track access to resources
- **Security policy** – maintain a security policy that addresses security
- **Physical security** – restrict physical access to locations storing data
- **Data encryption** – encrypt sensitive data in storage and transmission

5
★

# Encryption for data is Airbag for driver



6
★

# We recommend go ‘harder’ on encryption (South Korea example)

Why?

- When other cyber measures fail (like firewall) then last line of defense is unreadable data (that is encrypted data)
- Have higher level of encryption like folder and field level encryption
- Separate storage & management for Keys and Data
- Role separation – protect data from IT administrations
- Minimum access rights – control who has access to what, when & where
- Ever tighter encryption – start by locking the front-door, but plan to continue to tighten controls (lock room, then lock safe, etc..) as attackers will become more sophisticated over time. Current ransomware lessons

7
★

# Example of Fines

- GDPR fine of 4% of annual revenue or €20M (whichever is higher)
- Email, credit card data, health record per privacy standard – fines can be \$50 to \$100 per data element lost which can easily run into millions of dollars

8
★

**Example of encryption at every functional level, enabling you to implement protection-in-depth**

House Room Box Document

Sovereignty  
Confidentiality  
Integrity  
Availability  
Confidentiality  
Confidentiality  
Confidentiality  
Confidentiality  
Confidentiality  
Confidentiality

Encryption protects data at every functional level and enables you to implement protection-in-depth

Encryption protects data at every functional level and enables you to implement protection-in-depth

9 ★

**Problem example - Data is readable everywhere**

Data is readable to internal and external elements in Web, App and DB servers

Data in storage is not protected - data at rest is in clear text always

Data in transmission is not protected - data is in clear text always

Data in use is not protected - clear text data used without centralized privacy policy enforcement

"We are happy happy happy..."

10 ★

**Solution - de-identify data everywhere**

Data is de-identified and encrypted to internal and external elements in Web, App and DB servers

Data in storage is protected - data at rest is always de-identified format

Data in transmission is protected - data is always de-identified

Data in use is protected - de-identified data is revealed based on data & key policy

I am not happy

11 ★

**Protection application example servers - web, app, database, cloud VMs, containers**

Encryption

Access control for users and applications

Application blacklist

Application whitelist

Audit trail of every file access event

Centralized management

User

Ransomware

Any data  
Database  
Web  
App  
File

DPM Agent

12 ★

**Sovereign Core Data & Systems Infrastructures**

Fiji needs to identify critical Data & Systems Infrastructures:

- These are systems that are core to the Proper function of Fiji
- These systems must Protect our People
- These systems are important for the Prosperity of Fiji
- Designed and developed by a Core of Local Systems Designers and Developers
- Data must be domiciled locally
- Source Codes must be accessible to the Core Local Systems Administrators
- Foreign Systems Developers may be called in for Specific Duties but access to Source Codes must be carefully policed

13 ★

**Critical Core Data & Systems Infrastructure**

- Election Information Management System (EIMS)
- Immigration Management System (IMS)
- Births, Deaths & Marriages System (BDMS)
- Passport Management System (PMS)
- Judicial Management System (JMS)
- Police Intelligence & Law Enforcement Management System (PILEMS)
- Military Defence & Homeland Security System (MDHSS)
- Hospital Information System (HIS)
- Registrar of Companies Management System (RCMS)
- Registrar of Titles Management System (RTMS)
- Integrated Tax Information System (ITIS)

14 ★

**solé**

vinaka vakalevu

15 ★

**PIFS verbal submission to Fiji**  
**Standing Committee on Foreign Affairs and Defence.**

0935hrs 13 April 2023  
Fiji Parliament

- Thank you to the Chair, Honourable Viliame Naupoto, for the invitation.
- Introduction of Pacific Islands Forum Team, including Mr Paki Ormsby, Director of Policy, Mr Terio Koronawa, Regional Security Advisor, Mr Michael Crowe, Regional Security Advisor.
- The Pacific Islands Forum is the region's premier political and economic policy organisation. Founded in 1971, it comprises 18 members: Australia, Cook Islands, Federated States of Micronesia, Fiji, French Polynesia, Kiribati, Nauru, New Caledonia, New Zealand, Niue, Palau, Papua New Guinea, Republic of Marshall Islands, Samoa, Solomon Islands, Tonga, Tuvalu, and Vanuatu.
- The Forum's Pacific Vision is for a region of peace, harmony, security, social inclusion and prosperity, so that all Pacific people can lead free, healthy, and productive lives.
- The Pacific Islands Forum works to achieve this Vision by fostering cooperation between governments, collaboration with international agencies, and by representing the interests of its members.
- In July 2022, Pacific Islands Forum Leaders released the 2050 Strategy for the Blue Pacific Continent. The 2050 Strategy sets out the region's approach to collectively work together to achieve the long-term vision and aspirations of the 2050 Strategy, through seven key thematic areas.
- In terms of our discussion today, on cybercrime, two of those seven key thematic areas are directly relevant: the Thematic Area on Peace and Security, and the Thematic Area on Technology and Connectivity.
- In those sections, Leaders reiterated the expanded concept of security for the Pacific that had been defined in 2018, that includes cybersecurity, and shared a vision that 'all Pacific peoples benefit from their access to affordable, safe and reliable land, air and sea transport and ICT infrastructure, and systems and operations, while ensuring culturally sensitive user-protection and cyber-security.'
- In terms of regional security policy, the vision outlined in the 2050 Strategy builds on, and reaffirms, Forum Leaders' 2018 Boe Declaration on Regional Security.
- In the Boe Declaration, Forum Leaders outlined an expanded concept of security for the Pacific region. Recognising that among other challenges, cybercrime posed an increasing

threat to the safety and wellbeing of the Peoples of our Blue Pacific Continent, Leaders affirmed that cybersecurity was a priority security threat requiring concerted collective regional effort to address.

- The Forum Secretariat continues to assess that cybercrime, and cyber-enabled crimes, will continue to negatively impact the peace and prosperity of Pacific peoples, and that continued effort is required by all Members and partners to mitigate this threat.
- Following the Boe Declaration on Regional Security, in 2019, Forum Leaders endorsed the Boe Declaration Action Plan, which outlines a range of proposed actions to combat security threats, including a full strategic focus area on cyber threats.
- To address cybercrime, Forum Members committed to five key actions:
  - (i) Sharing information on cybersecurity and cybercrime threats through relevant fora such as the Pacific Cybersecurity Officials Network.
  - (ii) Supporting the development of national cyber policies/strategies and legislation,
  - (iii) Promoting awareness and educating our people on responsible cyber behaviour,
  - (iv) Developing and strengthening of computer emergency response teams, and last but not least,
  - (v) Promoting and supporting Forum Members' accession to the Budapest Convention on Cybercrime.
- Before I talk further on the Budapest Convention, I wish to highlight an underlying premise of regional security, recognised by Forum Leaders in the Boe Declaration on Regional Security. Namely that national security impacts on regional security.
- Noting this premise, Forum Members have committed to strengthening respective national security approaches, and thus contribute to security across the Blue Pacific Continent.
- In terms of cybersecurity, Forum Members have done this in a number of ways, in line with the Boe Declaration Action Plan.
  - Tonga, Samoa, Kiribati, Vanuatu and Papua New Guinea (to name just a few) have developed national computer emergency response teams.
  - Several Members have worked closely with the Pacific Islands Chiefs of Police Network to enhance cybersafety awareness with online-hygiene programs in schools and workplaces.
  - Vanuatu and Kiribati have developed national cyber security strategies, and all Forum Members, including Fiji, are sharing information on cybersecurity through the Pacific Cybersecurity Officials Network and the Pacific Transnational Crime Network.

- Finally, directly related to today's discussion, several Members have significantly progressed their efforts to accede to the Budapest Convention on Cybercrime.
- The Budapest Convention on Cybercrime is regarded by Forum Members as the most comprehensive and coherent international agreement on cybercrime and electronic evidence to date.
- It serves as a guideline for any country developing domestic legislation on cybercrime and as a framework for international cooperation between State Parties to the Convention.
- The Budapest Convention provides for:
  - (vi) the criminalisation of conduct – ranging from illegal access, data and systems interference to computer-related fraud and child pornography;
  - (vii) procedural powers to investigate cybercrime and secure electronic evidence in relation to any crime, and
  - (viii) for efficient international co-operation. The treaty is open for accession by any country.
- In terms of Pacific Islands Forum Members, Australia and Tonga have already acceded.
- Like Fiji, Vanuatu and New Zealand have been invited to accede by the current parties to the Convention, after indicating their interest in accession, following the drafting of laws that indicate they have implemented or are likely to implement the provisions of the Budapest Convention in domestic law.
- In the Forum Secretariat's view, Fiji's accession to the Budapest Convention would provide further momentum and inspiration for fellow Forum Members to continue their own national efforts to accede. We believe that acceding to the convention is not just in Fiji's interest, but by extension, it is in the region's interest also.
- We want the region to become a hard-target for cybercriminals.
- We want cybercriminals to know that if they perpetrate cyber-related fraud, crime, interference, forgery and trespassing anywhere in the Blue Pacific Continent's cyber domain, including in Fiji, they can and will be caught, tried and prosecuted.
- In concluding, we wish to highlight that the Forum Secretariat is aware of a range of support that is available to Forum Members to aid their effort to accede to the Budapest Convention and want to underscore that Fiji is not alone in its efforts to accede.
- The Pacific Islands Legal Officers Network hosts a Cybercrime Working Group, which brings Forum Members together to exchange information and lessons learned, including on Budapest Convention accession efforts.
- That network has a close working relationship with the Council of Europe (the host of the Budapest Convention) and facilitates assistance between the Council of Europe's

development assistance program (Global Action on Cybercrime Plus (GLACY+)) and Forum Members (as well as other developing nations the world over).

- The purpose of that program is to strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area.
- We understand Fiji has engaged with this program in the past and we have received indications from the Council of Europe that it intends to continue to support Forum Members with such efforts into the future.
- Further, just as we do for all our Members on a broad range of security issues, the Pacific Islands Forum Secretariat, your regional Secretariat, remains ready to assist in any way we can to support Fiji in its national security development efforts. This includes on cybersecurity, and this includes support in relation to your accession to the Budapest Convention.
- Finally, I wish to highlight recent comments from Fiji's neighbour, and fellow Forum Member, Tonga, who has already acceded to the Budapest Convention.
- While acknowledging that more work is still required to fully realise the benefits of accession to the Budapest Convention, the Attorney General of Tonga recently presented to fellow Forum Members that Tonga's accession to the Budapest Convention has afforded it an opportunity to align its domestic laws with that of the 67 countries worldwide who are leading the fight against cybercrime.
- By having laws that are better aligned with those 67 other countries, Tonga has a sound basis on which to build interoperability in dealing with the transnational nature of cybercrime.
- Until the whole region has acceded to the Budapest Convention, there will remain gaps in our ability to work together to prosecute cybercriminals. Fiji's accession and subsequent efforts will help fill one of those gaps, and thus make our region that little bit more safe and secure.
- Thank you Chair for the opportunity to make this humble submission to you today.

**25 April 2023**  
**By: Email**

Hon. Viliame Naupoto  
Chairperson  
Standing Committee on Foreign Affairs and Defence  
Government Buildings  
Suva, Fiji

Dear Sir

**RE: Written Submission on the Convention on Cybercrime**

I refer to the invitation for the Commission to provide an oral submission on the Convention to the Committee to assist on the inputs in reviewing the Convention on Cybercrime on whether Fiji should ratify the Convention (with or without reservations).

I am very pleased to confirm my attendance for Thursday, 27 April 2023 at 09.00am (Fiji Time) to present the following summary to the Standing Committee on Foreign Affairs and Defence.

1. The Online Safety Commission ('OSC') empowers Fijians to be responsible and safe online. It provides Fijians a space to resolve concerns with respect to online abuse such as online bullying, internet trolling or image based abuse.
2. The OSC provides an avenue to assist individuals confronted with harmful online content by delivering services and resources that help to minimise the harm and educate ways to be proactive and safe online. These include developing and designing educational content of online safety, organising awareness programs, receive and manage online abuse reports from individuals, provide access and advice in relation to queries submitted to the Commission, investigate online abuse reports through alternate dispute resolution mechanisms that would bring about efficient and reasonable means of redress or collaborate with relevant agencies and governments to provide the best possible outcome.
3. We understand the convention provides a framework for protecting individual rights in the context of cybercrime investigations and prosecutions. It requires signatories to respect fundamental rights, such as privacy, freedom of expression, and ensures that any measures taken to combat cybercrime are necessary, proportionate, and subject to judicial review.
4. While we commend the state for having national legislation such as the Online Safety Act, the recent Cybercrime Act and the Crimes Act that identify computer and cyber related crimes, being a part of this convention will also require some amendments to these established instruments in order for the convention to work in unity with established mechanisms.



5. Since establishment, the OSC has witnessed the rise of online abuse primarily as it relates between persons, such as cyberbullying, image based abuse, doxing and more. In light of these reports, it is clear that women and girls are disproportionately targeted and abused through online platforms and tools making them more susceptible to gender based online violence.
6. On January 14th 2020 the OSC signed a Memorandum of Understanding with the Fiji Police Force to assist in these specific forms of abuse and other related online abuses creating effective cooperation that is built on mutual trust, shared non privileged information, and investigating online abuse reports and seek to resolve those reports in a manner outlined by the Online Safety Act 2018.
7. This Budapest Convention serves to be an instrument that would allow such cooperation at a higher level. In light of this, it is important to remember the safety of the individuals rather than only focusing on the infrastructure or policies alone. With the effects of global cyber threats and attacks on critical sectors including finance, ICT, public safety, health, and e-government services; cybercrime requires a coordinated and comprehensive response. It has become apparent that criminals can easily operate across borders and without international cooperation, it would be difficult to investigate, let alone prosecute them.
8. By acceding to the convention, a country can benefit from an increased cooperation with other signatories and enhance its abilities to investigate and prosecute cybercrimes.
9. Given the above, the Online Safety Commission submits the following recommendation:
  - a. Fiji accede to the convention without any reservations;
  - b. Fiji carefully consider and amend relevant national laws including the Online Safety Act 2018 to work coherently rather than in isolation; and
  - c. Fiji clarifies the role and responsibility of existing law enforcement and state agencies in relation to this Convention.

Should you have any clarifications, please do not hesitate to contact the undersigned.

Sincerely,

A handwritten signature in black ink, appearing to read 'Tajeshwari Devi'.

Tajeshwari Devi  
Acting Commissioner  
Online Safety Commission

Slide 1

Ministry of Home Affairs and Immigration

**Presentation to the Standing  
Committee on Foreign Affairs  
and Defence**

Tuesday 2<sup>nd</sup> May 2023

**Slide 2**

## **CONVENTION ON CYBERCRIME (BUDAPEST CONVENTION)**

**Slide 3**

### **Scope**

- Background
- Summary of the Convention on Cybercrime (Budapest Convention)
- Fiji's Status
- Why Fiji should accede to the Convention
  
- Way Forward
- Questions

#### Slide 4

## Background

- 2010 Cybersecurity Working Group
- Cabinet Decision

#### Slide 5

## Summary and fundamental pillars of the Convention

1. Standardizing Cybercrime legislation
2. Capacity Building between law enforcement agencies
3. Strengthening international cooperation amongst State Parties

## Slide 6

### Fiji's Status

- In 2021, Fiji was invited by the Council of Europe to accede to the Budapest Convention. A convention that provides a comprehensive and coherent framework on cybercrime offences and electronic evidence.
- Fiji has partially adopted the Convention into its Computer Crimes Act 2009 and Cybercrime Act 2021

## Slide 8

### The nexus between Cybercrime and Cybersecurity

- Cybersecurity is a security thematic area.
  - *Cybersecurity is all about the various methods, technologies, processes frameworks, policies, strategies and legislations to help protect systems, networks against cyber-threats and attacks in cyberspace.*
- Cybersecurity threats always surfaces in the form of cyber-breaches that are reported to law enforcement.
- Government must take proactive measures to protect the country's cyber and data infrastructure and the cyber safety welfare of its citizens..
- Alignment of cybercrime legislation and cybersecurity with national security is critically important in this era of new and innovative technology.

## Slide 9

### Benefits to the Ministry of Home Affairs and Immigration

- Enhances the proposed National Critical Infrastructure Cyber Incident Response and Recovery Policy Framework
  - Critical Infrastructure Computer Emergency Response Team (CERT)
  - Critical Infrastructure Computer Security Incident Response Team (CSIRT) within CI agencies
- Enhances the effectiveness of incident response capability of CI CERT and CSIRT with nation states and multinational agencies through **International Cooperation**
- Ensures free flow of mutual requests and assistance through international co-operation and dual criminality

## Slide 10

### Re-Assignment of Cybercrime Legislation to the Ministry of Home Affairs and Immigration

- Fiji Police began Cybercrimes Investigations and Computer forensics in 2006 and Digital Forensics laboratory opened in October 2022
- Fiji Police Cybercrimes Unit continues to involve itself in areas that are affected by cyber-threats
- Fiji Police falls under the Ministerial Assignment of Minister of Home Affairs; it is kindly proposed that the Cybercrime Act 2021 be under the portfolio of the Minister of Home Affairs and Immigration

## Slide 11

# Way Forward

- To accede and ratify the Convention
- Working in collaboration with and Critical Infrastructure agencies  
-Formulation of a Cyber Security legislation and Framework which governs Critical Infrastructure agencies
- Transfer of Cybercrime Legislation 2021 to the Ministry of Home Affairs and Immigration

## Slide 12

# Any questions?

# Verbatim Reports

# **[VERBATIM REPORT]**

## **STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE**

### **Convention on Cybercrime**

**SUBMITTEE: UNIVERSITY OF FIJI**

**VENUE: Big Committee Room, Parliament**

**DATE: Tuesday, 20<sup>th</sup> September 2022**

**VERBATIM NOTES OF THE MEETING OF THE STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE HELD AT THE COMMITTEE ROOM (EAST WING), PARLIAMENT PRECINCTS, GOVERNMENT BUILDINGS ON TUESDAY, 20<sup>TH</sup> SEPTEMBER, 2022 AT 10.14 A.M.**

**Interviewee/Submittee:** University of Fiji

**In Attendance:**

- 1) Professor Shaista Shameem - Vice Chancellor
  - 2) Professor Aziz Mohammed - Lecturer (School of Law)
  - 3) Professor Shawkat Ali - Lecturer (School of IT)
  - 4) Ms. Varsha Bano - Criminal Law Expert
  - 5) Mr. Farik Mohammed - IT Expert
- 

DEPUTY CHAIRPERSON.- Honourable Members, Members of the Public, secretariat staff , ladies and Gentlemen: A very good morning to you all and it is a pleasure to welcome everyone, especially the viewers who are watching. At the outset, for your information, pursuant to Standing Order 111 of the Standing Orders of Parliament, all Committee meetings are to be open to the public. Therefore, please note that this submission is open to the public and media and is also being streamed live on Parliament's website and social media online platforms and the Parliament Channel on the *Walesi* Platform. For any sensitive information concerning the matter before us this morning that cannot be disclosed in public, this can be provided to the Committee either in private or in writing. However, please be advised that pursuant to Standing Order 111(2), there are only a few specific circumstances that allow for non-disclosure and these include:

- National Security matters;
- Third party confidential information;
- Personnel or human resources matters; and
- Committee deliberation and development of Committee's recommendation and reports.

I wish to remind honourable Members and our guests that all questions to be asked are to be addressed through the Chair. This is a parliamentary meeting and all information gathered is covered under the Parliamentary Powers and Privileges Act. However, please bear in mind that we do not condone slander or libel of any sort and any information brought before this Committee, should be based on facts.

In terms of the protocol of this Committee, please minimise the usage of mobile phones and all mobile phones to be on silent mode while the meeting is in progress. I would like to, at this time, introduce the Members of my Committee. Unfortunately our Chair, honourable Alexander O'Connor is away on

bereavement leave so I am chairing today's session. I am Dr. Salik Govind, the Deputy Chairperson of the Committee. Honourable Qereqeretabua is also unable to attend this morning's session.

*(Introduction of Committee Members)*

Today, the Committee will be hearing a submission on the Convention on Cybercrime, otherwise known as the Budapest Convention and for the purpose of the viewers that are joining us this morning, I would like to give a brief explanation on this Treaty. The Convention on Cybercrime, also known as the Budapest Convention provides a comprehensive and coherent framework on cybercrime offences and

1

electronic evidence. It serves as a guideline for any State developing comprehensive national legislation against cybercrime and as a framework for international cooperation among States Parties.

To date, the Convention has 67 member States, which includes Australia and Tonga from the South Pacific region. Pursuant to Article 37 of the Convention, any other State such as Fiji can become a Party by accession, if the State is prepared to implement the provisions of the Convention and upon invitation to accede to the Convention after consultation and approval of Parties.

With the extreme effects of global cyber threats and attacks on critical sectors such as finance, ICT, energy, water, emergency services, public safety, health, public services, aviation and e-government infrastructure, becoming a Party to the Convention will enhance Fiji's ability to combat cybercrime, with international support and assistance, particularly in relation to continued capacity building, to better equip Fiji's criminal justice authorities including the judiciary, prosecution and law enforcement agencies.

Before us we have the Vice-Chancellor of the University of Fiji, Professor Shaista Shameem.

Madam and senior faculty members of the Justice Devendra Pathik (JDP) School of Law are to introduce themselves and to begin their submission and after which, there will be a Question and Answer session. Please also note, if there are any questions by Members of the Committee, they may interject or will wait till the end of your presentation to ask the Committee questions. Thank you and you may start, Professor Shameem.

PROF. S. SHAMEEM.- Thank you very much, Deputy Chairperson and the honourable Members of the Committee of Parliament. We are delighted to be here this morning to make our small contribution to this particular subject which is in fact a very important one from both the laws aspects, as well as from technology. So in fact our team is made up of two schools, both the Schools of Laws, the JDP School of Law as well as the School of Science and Technology.

So, if you will allow me, Sir, I will introduce my team now.

*(Introduction of the representatives from the University of Fiji)*

PROF. S. SHAMEEM.- I will just be doing the introduction I cannot pretend to have expertise on the subject at all. So, my job is just to introduce them and then of course, if you would like to ask question afterwards, we will be happy or endeavor to answer them but if there are difficult questions because as you probably know, Deputy Chairperson, that we received the invitation to make submission about four or five days ago. So everyone has been working really hard putting the submission together. So, there may be gaps that you may perhaps, find that we will be very happy to respond to, should there be questions at a later date and we can work with the secretariat in that regard. So, that is what I need to say by way of introduction. May we proceed, Sir.

DEPUTY CHAIRPERSON.- Please start.

PROF. S. SHAMEEM.- Thank you very much. We will start with Ms. Bano.

MS. V. BANO.- Deputy Chairperson and Members of the Standing Committee, as part of our submission on legal issues, my colleague, Professor Mohammed and I will be raising two points. The first point which focuses on how Accession to the Convention would benefit Fiji by minimizing harm will be addressed by myself.

The second point which focuses on other related legal instruments relevant to the Convention will be addressed by Professor Mohammed. The effects of Cybercrime are well known, it not only causes financial loss but also threatens our peace and security. Cyber criminals take full advantage of the anonymity, secrecy and interconnectedness provided by the internet, therefore attacking the very foundations of our modern information society.

Investigating and prosecuting such offenders has become a challenge, particularly when an offender is located in a different country. This makes us realise how important it is to have in place laws that would allow effective international co-operation, especially when dealing with trans-border crime. Accession to the Convention would help Fiji address these issues, the principle aims of the Convention include:

1. Harmonizing the domestic, criminal substantive law elements of offences and collected provisions in the area of Cybercrime
2. Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences, as well as other offences committed by means of the computer system; and
3. Setting up a fast and effective regime of international co-operation.

Deputy Chairperson and honourable Members, we humbly submit that the Convention will undoubtedly aid Fiji in combatting Cybercrime related offences at an international level, by allowing neutral cooperation across territories.

We also submit that the Convention is a cybercrime treaty in title, but its benefit encompasses more. Its provisions deal with pure cybercrime, cyber enabled crime and criminal evidence stored electronically.

In acceding to the Convention, we will be required to incorporate the following into our domestic legislation:

- (a) Offences against confidentiality, integrity and availability of computer data and systems;
- (b) Computer related offences such as fraud or forgery;
- (c) Content related offences such as the distribution of child phonography through computer systems; and
- (d) Offences related to the commercial scale infringements of copyright and theft of intellectual property.

Currently, the Crimes Act 2009 specifically Sections 336 to 346 create computer offences, however these sections do not capture the complex and evolving nature of cybercrime.

We will also be required to establish search and surveillance powers necessary for obtaining electronic evidence of offending consistent with domestic and international human rights obligations. These include:

- a) Measures to order the expeditious preservation of subscriber data, traffic data and content data;
- b) Measures to order the production of the specified computer data and subscriber information;
- c) Measures to enable search and seizure of stored computer data; and
- d) Measures to collect traffic data associated with specified communications in real time and in relation to serious offences measures up to collect computer content data in real time.

The Convention includes provisions requiring that enforcement powers and procedures established under the Convention are to be conducted with adherence to fundamental human rights and freedoms, including freedom of expression, respect of privacy and personal data. This allows the ordinary public constitutional protection but at the same time, does not permit offenders to take refuge in impunity.

The Convention also sets out several principles and procedures related to international cooperation. These include:

- a) Procedures relating to mutual assistance and the collection and sharing of electronic evidence;
- b) The establishment of the 24-hour designated point of contact to ensure the provision of assistance between parties for the investigation of cybercrime.

Accession to the Convention would enhance co-operation with member states to address cybercrime. Fiji would need to make incremental amendments to its laws to accede to the Convention. These changes would complement and enhance Fiji's International Commitment on Cybercrime.

Mr. Chair and Members of the Committee, that is the end of my submission. I am happy to take any questions if Mr. Chair thinks fit.

MR. CHAIRPERSON.- Thank you, may be towards the end.

MS. V. BANO.- Thank you. May I now invite my colleague Professor Aziz Mohammed to submit on the second point.

PROF. A. MOHAMMED.- Mr. Chair, my submission is in relation to other instruments relevant to the Convention on Cybercrime. It is with respect we submit that the Convention on Cybercrime should not be seen in isolation but also consideration should be made to other impeding legal instruments that have been legislated and associates with the Convention on Cybercrime.

The first document we would like to refer to is the additional protocol to the Convention on Cybercrime.

This protocol concerns the criminalization of acts of a racist and xenophobic nature committed basically through the computer system. This additional protocol was the subject of intense negotiations from late 2001 and early 2002. The first text of this protocol was adopted by the Council of Europe that has been the proponent of this Convention of Cybercrime, the Committee of Ministers endorsed it on 7th November, 2002. This was done we all know, through the title "Additional Protocol to the Convention on Cybercrime".

The second document, I would like to refer to associated with the Convention on Cybercrime is the Second Additional Protocol to the Convention. This protocol enhances co-operation and disclosure of electronics that are utilised in the commission of undesirable acts.

The second protocol aims to further enhance co-operation on cybercrime and its ability of the criminal justice authorities to collect evidence in an electronic form that is associated with the criminal offence for the purpose of specific criminal investigations or proceedings through additional tools pertaining to a more efficient mutual assistance.

This mutual assistance and other form of co-operations between competent authorities, co-operation in emergencies (that being in situations where there have been significant and imminent risk to the life or safety of natural persons), and direct co-operation between competent authorities and service providers and other entities in possession or control of pertinent information. The purpose of this Protocol is to supplement the Convention and provide a better platform in its implementation.

We submit that in considering the implementation of the Convention, these two Protocols should be in addition to what will be considered for this purpose.

Deputy Chairperson, we would also like to draw the attention to more recent developments in this area. The third notable development in this respect is the proposed United Nations Treaty on Cybercrime. After years of discussion, the UN General Assembly has voted to begin negotiations on a Cybercrime Treaty that has potential to reshape policing on a global scale and we all know that this is more in relation to the serious implications in regards to human rights. UN Resolution 74/247 created the Ad Hoc intergovernmental committee with the draft proposed Treaty.

The Committee held its first negotiating session from 28th February, 2022 to 11th March, 2022. There seems to be support on the inclusion of what is termed as the pure Cybercrime Convention with the like network intrusion or interference with the operations of a computer system. Also for discussion are matters associated with broader range of 'cyber-enabling' crimes such as fraud or drug trafficking related matters that do not inherently target information and communication technologies but where Information and Communication Technologies become useful.

Deputy Chairperson, we submit that the Convention on Cybercrime, Additional Protocol to the Convention on Cybercrime, especially the First and the Second Protocols enhances co-operation and disclosure of electronic present no adverse provisions that would undermine any current domestic legislations. In fact, they will only be enabling. We should be cognisant of the fact that the third document we referred to the UN Treaty on Cybercrime adopted will again only enhance what our intentions are, in trying to thwart the very issue of cybercrime.

MR. F. MOHAMMED.- Through you, Deputy Chairperson and Honourable Members of the Standing Committee, good morning. The next part of our discussion is going to be in relation to the science and technology issue and Professor Ali and I will be taking us through this part. The discussions are going to be in relation to four quotes that are there.

For the first two quotes, I will be taking the honourable Members through and for the last two quotes, Professor Ali is going to take us through. Let me begin with the quote from General Sun Tzu, from the book *Sun Tzu in the Art of War*, which is the latest military treaties in the World and cyber security professionals take in the experiences from there to follow through in relation to mending security weaknesses:

“An army that is better prepared, that is highly trained, that fights an unprepared enemy, and one that makes no mistakes - is destined to win”

Deputy Chairperson, the cyberspace, better known as the internet, is a digital war zone, where cyberwars are fought continuously between the cybersecurity professionals and cybercriminals. As defenders, we know that the cybercriminals are from one of the several categories of unethical hackers – because there are also ethical hackers who assist us in defence. The unethical are the script kiddies, blue hat hackers, hacktivists, malicious insider or whistle blowers, state or nation sponsored hackers or black hat hackers. Each category of hacker is well trained and skilled for the specific missions they want to accomplish. Some common types of cyber-attacks include Denial of Service (DoS), Distributed Denial of Service (DDoS), Man-In-The-Middle (MITM) Attack, phishing attack, whale phishing attack, spear phishing attack, Ransomware Attacks, Password Attacks, Structured Query Language (SQL) Injection Attack, which attacks databases, Uniform Resource Locator (URL) Poisoning Attack which affects websites or anything to do with the https protocols, Domain Name System (DNS) Spoofing, Session Hijacking Attacks, Brute Force Attack, Web Attack, insider threat, Trojan horse, drive-by Attack, Cross-site Scripting (XSS) Attack which relates to Website Attacks, Eavesdropping Attack, Birthday Attack, Malware Attack and the list just goes on and on with the new technologies and new frontiers appear in science and technology.

In a cyberwar, an attacker may only need one successful attack to win, but defenders need to be successful against all attacks to win, because one successful attack may be enough to do the damage. Second quote:

“Rely not on the likelihood of the enemy not coming or attacking, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.”

All apps (applications) which relate to applications or software, websites and Application Programming Interfaces (APIs), which are used as tools to connect our software together on information systems as well as the entire information system need to be securely developed. Secure Software Development Life Cycle (SecSDLC) model is a new tool for software development from the area approach which was not so secure. This model must be used for all software engineering projects. In SecSDLC, security is integrated in each phase of the software development life cycle and there are six phases. This is so that security gets built-in from the very core of the system and not left to be considered as an afterthought just like previously SDLC used to take in for granted.

It is important to identify and fix vulnerabilities also. All information systems that render critical services are also made up of components such as hardware, software, networks, procedures, data and people. These are the mix of components which make our information system available and do the work or the service which it is supposed to provide. Each of these components must be secured against critical and highlevel vulnerabilities. Network defenders can use network vulnerability assessment software tools such as Tenable Nessus to identify critical, high-level as well as low-level vulnerabilities (weaknesses) in our systems. These systems, for example, the software systems are in relation to operating system, applications software and the network protocols in use that relate to the imminent threat.

The resulting report can be used to provide necessary fixes in relation to the imminent threat to neutralise the resulting attack as well as the associated risk posed by those attacks. Moreover, most vulnerabilities in software and hardware can be eliminated by upgrading to the latest version or applying software or firmware updates and the hardware. Also Fiji should not allow technology sellers to import obsolete and insecure software or endpoint devices and network technologies into the Fiji market. Such technologies will only make the fight against cyberattacks more difficult.

The internet is a powerful vehicle for many services that benefit humanity. Accessing e-government services, social networking, emailing, web browsing, web search, remote working, online studies, eshopping, e-banking, e-payments and mobile top-up are some of the most common activities that people in Fiji use the internet for. However, the internet is also a Pandora's box through which hackers target the confidentiality, integrity, and availability of data and critical services. For example, if an SQL injection attack succeeds, several things can happen including the release of sensitive data or the modification or deletion of important data. We need to develop secure databases and data entry forms, implement encryption to ensure confidentiality of Personal Identifiable Information (PII), develop better and use better hash algorithms to ensure integrity of data, and implement robust distributed systems and backup systems to ensure 24-7-365 availability of information and critical services from our network infrastructures.

Also in the mix is a White Hat Hacker. A White Hat Hacker is often contracted by businesses as a penetration tester to perform further security tests by trying to actively penetrate system weaknesses. This tester then reports back to the business explaining how bad the situation is and if anything requires fixing, the tester guides how to fix the problem, so that is the good guy.

When a vulnerability is fixed in time the related threat is neutralised and the related attack will not pose risk. For example a penetration tester may send a tempting phishing email to test end-users (the people or human resources who can fall victim to the attacks) those who click on the link are identified as the vulnerable people in the system who need urgent cybersecurity awareness training against phishing attacks.

So training can be provided to that group of people so that they become more aware and prevent such kind of attacks. When people are aware about how to inspect emails for example, for signs of phishing can positively identify an email as phishing email and then does not action that attacker's link on the message, that kind of attack is neutralised.

Also to reduce the risk of insider attacks, the principle of least privilege also called least privilege access is implemented so that the user only has access to what he absolutely needs to perform those responsibilities and no more. For secure procedures, defenders should utilise international standards such as ISO/IEC 27001 which relates to Information Security Management, ISO/IEC 27002, ISO/IEC TS 27100 which is Information Technology Security and ISO/IEC TS 27110 which relates to Information Technology, Cybersecurity and Privacy Protection. Correct application or implementation of these standards ensures that our information systems have adequate controls in place for cybersecurity.

Deputy Chairperson, Sir, that is my presentation and I will let Professor Ali to continue. Thank you.

PROF. S. ALI.- Deputy Chairperson, honourable Members of Parliament, the Vice Chancellor, good morning. I would like to share Philosopher Sun Tzu quotation and I quote,

"Being skillful in attack means that the enemy does not know what to defend and being skillful in defense means that the enemy does not know what to attack."

Cybersecurity is a game of attack and defense, to defend against cyber-attacks one needs to think like an attacker, every attack is carefully planned because they are coming and intelligent too and execute using the attack model, Cyber-Kill Chain.

Step 1 - Reconnaissance phase of Cyber Kill Chain, the attacker probes for a weakness. This might include harvesting login credentials or information useful in a phishing attack.

Step 2 - Weaponization phase, the attacker builds a deliverable using an exploit and a backdoor.

Step 3 - Delivery, the attacker sends the weaponized bundle to the victim. For example, sends a malicious link in a legitimate looking email.

Step 4 - Exploit phase, the malicious code is activated and executed on the victim's system.

Step 5 - Installation phase, the malware is installed on the target asset.

Step 6 - Command and Control (C&C) phase, a channel gets created for the attacker to control the system remotely.

Step 7 - Action phase, the attacker remotely carries out his intended goal. Just like the attackers, the defenders can also use the Cyber Kill Chain to test their system for security weakness.

Moreover, cybersecurity can be strengthened by applying defense-in-depth and layered security mechanisms. Layered security is implementing multiple products to address one single aspect of security.

Using seemingly redundant products strengthens the enterprise's defence against threats, for example, a gateway and a firewall both determine which data should be allowed to enter the network. There are certainly differences between the two - a gateway is hardware while a firewall is both hardware and software but they both aim to restrict access to certain websites and applications.

Once the gateway and firewall have done their jobs an employee has been allowed to visit a particular website, for example, another security product or service will have to take over if the employee wants to enter a password to log in to that website.

The next security product can be Multi Factor Authentication (MFA) (this is completely new but popular) which prevents access to a website unless multiple credentials are provided. In other words, layered security only addresses one dimension of security or one vector of attack while defense-in-depth is broader, multi-faceted and more strategic in scope.

A layered security strategy is implemented using three different controls:

- i) Administrative; ii)
- Physical; and iii)
- Technical.

Administrative controls include the policies and procedures needed to restrict unauthorised access such as Role-Based Access Control (RBAC) or employee training to protect against phishing scams.

Physical controls incorporate physically securing access to the IT system such as locking server rooms while technical controls include the mix of products and services the organisation selects to address security. Core layers to carry out a defence in depth strategy should include:

1. Strong complex password;
2. Antivirus software;
3. Secure gateway;
4. Firewall;
5. Patch management;
6. Backup and recovery;
7. The principle of least privilege or giving a user the minimum access level or permissions needed to do his or her job.

Then as companies grow and the number of devices, applications and services used across the organisation increase, these serve as important security layers in a defence-in-depth strategy such as applying:

1. Two-factor authentication (2FA) or multi-factor authentication (MFA);
2. Intrusion detection and prevention system (and it works in this area very efficiently);
3. Endpoint detection and response (EDR);
4. Network segmentation;
5. Encryption; and
6. Data loss prevention (DLP).

A quote from Sun Tzu:

“If you know the enemy and know yourself you need not fear the result of a hundred battles. If you know yourself but not the enemy for every battle gained you will also suffer a defeat. If you know neither the enemy nor yourself you will succumb in every battle.”

With the right cybersecurity awareness, training skills and experiences Fijians can win against sophisticated cyber-attacks. However, as new technologies emerge, new threats and vulnerabilities will emerge and defenders will need to learn new ways to defend as adversaries learn new ways to attack.

Thus membership of Convention on Cybercrime will allow Fiji to gain from experiences of international partners in the fortification and development of secure digital infrastructure in the battle against cybercrimes in Fiji.

If you have any question my pleasure to answer that.

PROF. S. SHAMEEM.- Thank you very much, Mr. Chair and Members. We are now open to questions if you would like to ask anything specifically and if we cannot answer then we will return with response in due course.

DEPUTY CHAIRPERSON.- Thank you, Professor Shameem and your team. I think your presentation has been very, very useful. We intend to invite the University first because as Committee we really wanted to gain knowledge about the Cybercrime and also how the Cybercrime prevention and processes can be in place. What you have presented to us gives us a lot of insight on this topic of Cybercrime.

I have a question: at your institution (University) level, what kind of strategies you have in place to prevent any sort of cybercrime incident? Are there some specific things that the university is doing or what have you done to prevent cybercrime?

PROF. S. ALI.- Thank you Deputy Chairperson, it is definitely a good question. We are running cyber security courses in terms to add technical skills to our graduates. My colleague, Mr. Farik Mohammed is also responsible for these courses as well. I am teaching Artificial Intelligence (AI) which is very powerful tool and technology you know to protect. As Mr. Farik Mohammed had mentioned it is very difficult to figure out very recent attack. As I mentioned in my document, the people who are attacking our system are honestly smart and clever, smart people find it easy to identify all sorts of tricks they are applying. That is why we have to apply AI mission which is faster than human action. This kind of basic knowledge in cyber security network on how we can protect including suicide prevention awareness we are teaching our students at the University of Fiji.

DEPUTY CHAIRPERSON.- What sort of surveillance system you have in place? What kind of watchdog or surveillance are there to really identify if any such incident happens?

PROF. S. SHAMEEM.- I think perhaps, Deputy Chairperson, what you are asking the university as an institution, what it has in place in order to protect because we have got experts here and if we are not protected then our graduates would know but the university itself and I can tell and can give you assurance that in my experience with the university since 2009 (with a short lull in between) that we have not

experienced any of these attacks that my colleagues have been talking about and that is because we have stayed one step ahead of the game.

I believe that institutionally it is easier to be protected because the institutions have the money to make sure that they have the security systems in place. For individuals it is a lot harder. We have all the experience of somebody, for example, through the email saying 'I am a friend of yours', the name is used where a person is saying, 'please, deposit some funds, I am stranded in some country' et cetera and that is a hacking experience, I am sure as an individual to do that because our own individual systems are not protected because we just do not have the funds individually to protect. But for institutions if they do not put their mind and energy to it and their systems are hacked then they really, in a way, only have themselves to be blamed. They must stay ahead of the game.

A very good IT system within institutions is really important. A group of people who are not only doing but also helping staff through technology issues like, for example, with us teaching and learning; we have a new system or platform called 'Top Hat' that we use in our teaching which is a specific one because as a result of COVID-19 realities we realise that Moodle was not sufficient, so we actually purchased a system or platform so that has inbuilt protection and provide security to the students as well as the staff, because intellectual property (IP) rights is very important as well in trying to protect your IP rights and privileges from anyone who could access your system. The University does not have that experience yet but I do know that other institutions might have and they could talk about their own experiences but so far we have not. That just means that whatever little funds we have got and the University is not funded very well but whatever little funds we have got, we have been able to ensure that our security systems are in place. This is why we are very keen to make a contribution to this Standing Committee because we felt that acceding to the Treaty will provide us at nationwide level a bit more support in terms of the protection on cybersecurity issues. So I hope that answers your question.

DEPUTY CHAIRPERSON.- Yes, thank you very much. Can I open the floor for other honourable Members to ask questions?

HON. P.W. VOSANIBULA.- Deputy Chairperson on criminal law, as you have mentioned that the current law dealing with cybercrime, criminal law of 1979 is not so broad to cover what we have at the moment. I think in 2020 and 2021 the Standing Committee on Justice, Law and Human Rights conducted consultation throughout the country on our proposed Cybercrime Bill 2020. My question is: was the University invited on this consultation process?

PROF. S. SHAMEEM.- Yes, we were part of the consultation.

HON. P.W. VOSANIBULA.- Thank you. Why I am asking the question is because I am just reading the report and so important information you have provided this morning regarding the law on cybercrime.

HON. S. ADIMAITOGA.- Through you, Deputy Chairperson, I would like to thank you for your submission today. It has been very educational and empowering too. I love the part that has been quoted from General Sun Tzu in the *Sun Tzu in the Art of War* - If you know the enemy, you know yourself. I believe we need to have more awareness, we need to be empowered, not only from the institution like the University, individuals should learn too on this because when we are tagged, especially in cybersecurity, when they hack, we do not even know what to do. But then from your institution, I believe our students know more about it but we the public need to be empowered too on this so that we can know how to be protected and if we can know our enemy, to know ourselves and we do not have to fear the result of hundred battles. Thank you for your submission - very empowering.

DEPUTY CHAIRPERSON.- I have one question: There are other academic institutions like USP and FNU, do you have some kind of collaborative mechanisms to discuss the subject?

PROF. S. ALI.- Of course, in our advanced technology especially, we have to share. So recently in one of the projects we are running I can share through you since you are well informed, so we have got a project from Australia and Fiji and we built a project together: University of Fiji is a partner, the Monash University is a partner and the Queensland University is a partner as well so we have got funding as well to run this project. Our aim is to establish the Blockchain Model in the Pacific. This technology is a very brand new technology which, if you can implement then we can secure our Fijian communities in many ways. I can give an example: Blockchain technology is a very much distributed database, for instance, I have \$5,000 at Westpac and Westpac is carrying this information in my account, however, in other places I have noted this amount as well.

If the hacker takes \$1,000 from this account, the hacker may change this information but the other places, they cannot. It is very difficult to ....

From that point of view, our AI system can give the warning 'Ok something happened' then we can take action or AI can take action itself. That kind of project, I believe we are the only university in Fiji doing this with international collaboration, partners like Australia, U.S., Hong Kong and Singapore. Thank you, Chair.

DEPUTY CHAIRPERSON.- Good, excellent! Do you have any comments?

PROF. S. SHAMEEM.- No, Sir. I think if you are satisfied with those responses then we can leave it there. Subsequent to this, if you have further questions, honourable Chair and Members, we will be very happy to answer them. I am sure there would be some follow-up questions as you think about them. I must say that this is a very complicated subject and it is not in my field necessarily which is why we have the experts from the science and technology schools here so we do have expertise at the University of Fiji. Should there be any question either on science and technology side or the tech side or in the legal side, you mentioned the Cybercrime Bill, that would be something that we will be very happy to look into and research and get back to you.

We take the opportunity, Sir, to also say that the University of Fiji always looks forward to invitations from standing committees and select committees to provide submissions. We may not be able to do it as quickly as perhaps Parliament would like but we do our best to provide any kind of assistance we can. The University of Fiji has a new strategic plan, next five-year strategic plan (from 2022 to 2026), it is on our website.

One of the important missions of the University is to ensure that we are not only future-ready in terms of our content but also that we are a think tank for any organisation or Parliament or sub-committees that we can possibly be. We do not have the expertise on everything but whatever we can provide, we will be very happy to do so Sir.

DEPUTY CHAIRPERSON.- Thank you very much. Are there any other questions, no. Alright, please yes, feel free.

HON. S. ADIMAITOGA.- Thank you. I have read this:

‘Accession to Convention would enhance cooperation with member States to address cybercrime. Fiji would need to make incremental amendments to its laws to accede to the Convention.’

With this submission, I believe we are getting on towards that, for ratification and I believe we need to read this through because it empowers us too.

Further to that, we need to have more connection with the members from USP so that we can know how to handle this and how to ratify this Convention because I believe it is quite new but it has come on in Year 2021 but we need more interaction with you people so that we can try to amend this because it needs ratification so we need to be empowered on this topic. The more interactions we have with the members from USP, the more we will learn about it and then we can take it up to the next level. Thank you.

PROF. S. SHAMEEM.- Thank you and the University of Fiji.

HON. S. ADIMAITOGA.- University of Fiji. Thank you. I think they are very powerful too.

PROF. S. SHAMEEM.- Thank you so much. We will be delighted to assist in any way we can. I agree with you, Madam, that this is a difficult area and we need to know more about it because every day it changes, and that is the fearful part of it, and I think the quotations, as you correctly picked up, actually give us an idea about how we can be prepared for it. Internet and the technological world that we live in force us into that space to protect ourselves and I think Fiji as a nation, not just institutions individually or universities or organisations, but Fiji as a nation needs to protect itself as well. Thank you, Sir.

DEPUTY CHAIRPERSON.- Thank you. Professor Aziz, would you like to ....

PROF. A. MOHAMMED.- Sorry, Madam. May I? Madam, thank you for raising the very issue of enriching our community in regards to the understanding not only in Cybercrime but the development of laws that happen in other jurisdictions and outside Fiji.

I think the comfort we have is having eminent personnel like our Vice Chancellor leading a University and pushing all of us and actually challenging us to be here in such forum to share ideas.

I think what better than having her and letting me drop this idea that there may be some consideration of setting up a think tank and some affiliations with the University of Fiji.

In other jurisdictions this is the common practice and we have been strong advocates in terms of advocating about laws, not only that, in terms of human rights, human security and all other aspects that encompass the day to day affairs of our community.

So that is something that the Committee may want to consider and look at basically aligning with the University of Fiji in terms of future workings.

DEPUTY CHAIRPERSON.- Yes, I think once we ratify this Convention and work towards implementing, domesticating and getting a Bill which is in draft stage, passed then I am sure there will be a lot of opportunities to collaborate and it looks like you are already well-ahead with other institutions. I am sure there will be opportunity to collaborate especially in terms of capacity building which you have already started doing.

So when we come to implementing the law which will be following this then I am sure we will be having consultations.

At this juncture if we do not have any more questions, I would like to thank you all for availing yourselves this morning and providing us with such great knowledge which we are not aware of and that has really enriched our thinking and that will help us in formulating a report for Parliament to ratify this and also some recommendations for the future.

So once again I would like to thank you, Professor Shameem and your team. You always bring all your team members together which is great and we hope that in future we will continue to collaborate with you on other subjects.

With this, while we are transiting through the post COVID-19 period, we hope that together we can build a safe, secure and stronger Fiji and collaboration like this is very important for us the Standing

Committee of Parliament. So thank you very much and we wish you a safe journey back home. Thank you.

The Committee adjourned at 11.13 a.m.

# **[VERBATIM REPORT]**

## **STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE**

### **CONVENTION ON CYBERCRIME**

**SUBMITTEE: MINISTRY OF COMMUNICATIONS**

**VENUE: Big Committee Room, Parliament**

**DATE: Monday, 26th September, 2022**

**VERBATIM NOTES OF THE MEETING OF THE STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE HELD VIRTUALLY IN THE COMMITTEE ROOM (EAST WING), PARLIAMENT PRECINCTS, GOVERNMENT BUILDINGS ON MONDAY, 26<sup>TH</sup> SEPTEMBER, 2022 AT 9.58 A.M.**

**Interviewee/Submittee:** Ministry of Communications

**In Attendance:**

- |    |                      |   |  |
|----|----------------------|---|--|
| 1) | Ms. Tupou Baravilala | : | Acting Permanent Secretary                   |
| 2) | Mr. Shivendra Deo    | : | Director - Digital Government Transformation |
| 3) | Mr. Vijendra Singh   | : | Director - Digital Government Transformation |

Office of the Solicitor-General

- |    |                   |   |                   |
|----|-------------------|---|-------------------|
| 1) | Ms Glenys Andrews | - | Principal Officer |
|----|-------------------|---|-------------------|

Cybercrime Programme Office of the Council of Europe (C-PROC)

- |    |                    |   |                 |
|----|--------------------|---|-----------------|
| 1) | Ms. Catalina Stroe | - | Project Manager |
|----|--------------------|---|-----------------|
- 

MR. CHAIRMAN.- Honourable Members, members of the public, the secretariat, ladies and gentlemen; a very good morning to you all and it is a pleasure to welcome everyone, especially the viewers that are watching the proceedings.

For your information, pursuant to Standing Order 111 of the Standing Orders of Parliament, all Committee meetings are to be open to the public. Therefore, please, note that this submission is open to the public and media, and is also being streamed live on Parliament's website and social media online platforms and the Parliament channel on the *Walesi* platform. For any sensitive information concerning the matter before us this morning that cannot be disclosed in public, this can be provided to the Committee either in private or in writing. Please be advised that pursuant to Standing Order 111(2), there are only a few specific circumstances that allow for non-disclosure and these include:

1. National security matters;
2. Third party confidential information;
3. Personnel or human resource matters; and
4. Committee deliberation and development of Committee's recommendation and reports.

I wish to remind honourable Members and our guests, that all questions to be asked are to be addressed through the Chair. This is a parliamentary meeting and all information gathered is covered under the Parliamentary Powers and Privileges Act. However, please, bear in mind that we do not condone slander or libel of any sort, and any information brought before this Committee should be based on facts.

In terms of the protocol of this Committee meeting, please, minimise the usage of your mobile phones and all mobile phones are to be on silent mode while the meeting is in progress. I would like to take this time now to introduce Members of my Committee:

*(Mr. Chairman introduces Committee Members as well as Committee and Hansard Staff.)*

MR. CHAIRMAN.- Unfortunately, my Deputy honourable Dr. Salik Govind is unable to be here with us this morning as he is attending a bereavement in New Zealand.

Today, the Committee will be hearing a submission on the Convention on Cybercrime otherwise known as the Budapest Convention. For the purpose of the viewers that are joining us this morning, I would like to give a brief explanation on the Treaty, the Convention on Cybercrime (also known as the Budapest Convention) provides a comprehensive and coherent framework on Cybercrime offences and electronic evidence. It serves as a guideline for any State developing comprehensive national legislation against cybercrime and as a framework for international cooperation amongst States Parties.

To-date the Convention has 67 member States which include Australia and Tonga from the South Pacific region. Pursuant to Article 37 of the Convention any other State such as Fiji can become a party by accession if the State is prepared to implement the provisions of the Convention and upon invitation to accede to the Convention after consultation and approval of Parties with the extreme effects of global cyber threats and attacks on critical sectors such as Finance, ICT, Energy, Water, Emergency Services, Public safety, health, public services, aviation and e-government infrastructure. Becoming a party to the Convention will enhance Fiji's ability to combat cybercrime with international support and assistance particularly in relation to continued capacity building to better equip Fiji's criminal justice authorities including the judiciary, prosecution and law enforcement agencies.

Before us this morning, we have the Ministry of Communications, the Solicitor-General's Office and joining us virtually online is the Cybercrime Programme Office of the Council of Europe (C-PROC) and now I take the opportunity to ask Madam Acting Permanent Secretary to introduce the team. Before doing that, any questions will be left till after your submission and the floor is yours Madam. Thank you.

MS. T. BARAVILALA.- *Bula vinaka* Mr. Chairman, Sir, and honourable Members of the Standing Committee. Just by way of introduction, my name is Ms. Tupou Baravilala and I am the Acting Permanent Secretary for the Ministry of Communications and I would like to invite my colleagues if they could please also introduce themselves, maybe starting with the Office of the Solicitor-General.

MS. G. ANDREWS.- Good morning Mr. Chairman, Sir and honourable Members of the Standing Committee. My name is Ms. Glenys Andrews and I am a Principal Officer from the Office of the SolicitorGeneral.

MR. S. DEO.- Good morning Mr. Chairman, Sir, and honourable Members. I am Mr. Shivendra Deo, the Director Digital Government Transformation with the Ministry of Communications' part of the Digital Government Transformation Office.

MR. V. SINGH.- Thank you Mr. Chairman and Honourable Members of the Standing Committee. My name is Mr. Vijendra Singh and I am the Director Digital Government Transformation.

MS. T. BARAVILALA.- Mr. Chairman, Sir, I would also like to invite Ms. Catalina Stroe. I am not sure whether she has also introduced herself but maybe formally since we have started the proceedings. Ms. Catalina if you could please take it away. Thank you.

MR. C. STROE.- Thank you very much Ms. Tupou and good morning Mr. Chairman, Sir, and honourable Members of the Committee. I am Ms. Catalina Stroe. I am Programme Manager with Cybercrime Programme Office of the Council of Europe (C-PROC), I am managing and hoping to get another colleague of mine on one global project called Global Action on Cybercrime Extended (GLACY) and we have the pleasure to lead the counterparts in Fiji started some months ago when we initiated the huge work that lies in front of us and with respect to which I will be of any assistance in case you have questions for me afterwards. Good morning again and thank you.

MS. T. BARAVILALA.- Mr. Chairman, Sir, may we begin with our submission, thank you.

Firstly, Mr. Chair and Members it is indeed our pleasure to have the opportunity to present or reiterate our support for Fiji's Accession to the Budapest Convention and I am sure I not only speak on behalf of the Ministry of Communications but I am sure my colleague Ms. Glenys Andrews from the Office of the Solicitor- General and Ms. Catalina Stroe will also be in agreement so thank you for this opportunity. We are ready to answer any questions and I understand, Mr. Chair that this would be done at the end of our presentation.

Just with regards to the submissions we will be dividing these in three parts. I will be making sort of open it up with a few remarks. Our submissions will be based on the written analysis that was initially submitted when the motion was tabled before Parliament. I will then invite Ms. Glenys Andrews from the Office of the Solicitor-General to give a legal perspective and then I will invite Ms. Catalina Stroe to be able to provide a bit of context in terms of support being given to member States who are thinking of acceding too and also who are also already members of the Budapest Convention.

To begin with, I mean it is quite clear, Mr. Chair, and you have mentioned this in your opening remarks as well that technology continues to be sort of the main catalyst for change in the world and we have seen this as well. We have seen a lot of Fijians being online being connected and the internet has really become an intricate part of our lives and that dependence will continue to grow and we see that and also technologies will continue to evolve.

So when we look at quantum computing, robotics, artificial intelligence and even the Internet of Things (IOT) this is what we see when your fridge can then speak to the particular supermarket to say that you have a few groceries that it lacks then you have that being sent and delivered to your doorstep and all of that is done online.

So a lot of our lives have shifted dramatically into online spaces. We saw that with Fiji as well where we saw that when the pandemic came there was also a 23 percent surge and we continue to see this to grow.

Fijians we have seen have rightfully seized the opportunities that it presents. What we have also seen is that these increased opportunities have also presented or increased our threat landscape and that is exactly why it is critically important that we take priority to international instruments such as this.

Similar to that what we also see is (and we advocate for it) ensuring that all Fijians are safe online is a shared responsibility. So all of us - every stakeholder, has a role to play in this.

Furthermore, given the transnational the evolving nature and the unpredictable nature of Cyberspace international cooperation is imperative.

That leads me to our second point which is - why is this Convention important for Fiji?

The first and foremost reason is that this is the only legally binding international instrument on cybercrime and electronic evidence. So it really is the gold standard.

Mr. Chair, you did mention this was opened for signature in Budapest in November of 2001. It has been over 20 years and it still remains the most relevant international agreement when it comes to international cooperation and Ms. Catalina Stroe, I am sure will speak about this with regards to the membership that continues to grow improving the quality of the implementation and the level of cooperation between the parties.

The treaty itself is also evolving to meet new challenges and we see this with the first additional protocol and the second additional protocol which was recently opened for signature earlier this year as well.

There is a global increase of cyber attacks and we see this, I am sure, Mr. Chair and honourable Members whenever you may look online and you see that there is a lot of these attacks happening, it is becoming more sophisticated, we see a lot of zero-day attacks and it is becoming more common. You would have a cyber attacker that is in country A, they are using servers in country B and then you have victims in country C. So there needs to be rapid response across all enforcement agencies to be able to combat cybercrime and be able to do effective investigations and prosecutions of those cyber criminals.

What we have also seen is that the targets are across the wide spectrum, so from member States to companies all the way to critical infrastructure and critical information - infrastructures right down to families and individuals. We see this with even phishing attacks that are still taking place.

Mr. Chairman and honourable Members, what we are advocating for is that, this Convention really will enable us to more effectively combat cybercrime. It will increase our international collaboration and we have 67 member States that are already parties to this Convention and so you have a lot of these technology service in these various countries. The US, if I could quote one example, was actually part of the drafters of the Convention in 2001 and remains a party and so for us a lot of the data that we have, you may see some of these servers in all of these countries and so we really need that collaboration that is there on various levels from search which are our computer emergency response teams all the way up to collaborating with private sector or the technology giants.

The third element is to build that capacity across all the relevant stakeholders to ensure that we are bolstering our cybersecurity and cyber resilient efforts.

The third part of my remarks, Mr. Chairman would be really just to hone in on, I see that we are doing three today, so the three main benefits that we see that Fiji will be able to feel very tangibly when we do accede to the Budapest Convention and we are already seeing that now as well just being part of the priority group for capacity building.

The first one is that we are able to participate in projects of global capacity building. Catalina would have mentioned this earlier where we had the team actually come down. Experts in this were made up of prosecutors and judges and we dedicated trainings for the Judiciary, Law Enforcements and even up to the service providers.

So being able to have that training that took place where they were able to then share their learnings and share 'Look, this is how we are actually implementing the provisions or the Articles of the Budapest Convention' and talking about cases where they have actually used those collaborative mechanisms and tools that are in the Budapest Convention.

The second is the 24/7 focal points and this is highlighted in the Convention itself. As we have been seeing, all it takes is a few key strokes from one side of the world to be able to have consequences in a different time zone in a different country so rapid response is critical and what it allows for when we do accede is that, there needs to be 24/7 focal points in all of the member States so that if any issue happens, any need for investigation, all we need to do is call that person and say, "Hey I am having issues, I need you to quickly help" and we are 67 parties already and we have a number of countries including Fiji that are really trying to sign up as well. So that is a real great benefit for us particularly because Fiji and other small developing States we are technology takers so being able to have access to that and being able to have access to that expertise is something that will benefit us and help our criminal justice authorities to

be able to expedite the work and the investigations they are doing which leads me to my third point in terms of benefit is better collaboration with technology giants.

We have seen this even with the work that we have been doing, capacity building with Council rep but also in terms of our other development partners is being able to shape the conversations that are happening and making sure that our interests are also reflected in that.

Mr. Chairman, this is just a small brief overview in terms of really why we should be doing this and I think a lot of work really has been taking place behind the scenes. As you had noted, Mr. Chairman, this is not like a normal sort of treaty where if we would like to ratify or accede we just go ahead, we had to be invited to accede and I think working very closely with the Council of Europe in terms of taking the necessary steps, our Cybercrime Act 2021 which is aligned to the Budapest Convention provisions really put us in a great footing for us to be able to bolster our cyber security and cyber resilient efforts and really help in terms of the other things that we are doing with our other partners as well. I leave that at that, Mr. Chairman, and I would like to hand over to Ms. Glenys Andrews to take us through the legal provisions. *Vinaka.*

MS. G. ANDREWS.- Mr. Chair, through you, I will just take this Committee through the summary of the Convention as submitted in our written analysis, if that is okay?

The Budapest Convention or the Convention on Cybercrime as it is formally known as, contains a total of 48 Articles.

In summary, Article 1 of the Convention comprises the specific definitions of the terms: “computer system”, “computer data”, “service provider” and “traffic data”.

At this point, I would like to highlight that the Convention provides a mixture of requirements both legislative as well as procedural as you would have seen throughout the Convention.

The requirements under the Articles of the Convention are at a minimum for Fiji in order to be invited as we have been to be a party to this Convention.

Article 2 of the Convention requires each party to adopt legislative and other measures to establish as criminal offences when committed intentionally, the access to the whole or any part of a computer system without right.

Article 3 of the Convention requires each party to adopt legislative and other measures to establish as criminal offences when committed internationally, the interception without right made by technical means of non-public transmissions of computer data to, from or within a computer system.

Articles 4 and 5 of the Convention require each party to adopt legislative and other measures to establish as criminal offences when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right and the serious hindering without right of the function of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 of the Convention requires each Party to adopt legislative and other measures to establish as criminal offences misuse of devices.

Article 7 requires each party to adopt legislative and other measures to establish as criminal offences when committed intentionally and without right the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that the data be considered or acted upon for legal purposes as if it were legal.

Article 8 of the Convention requires each party to adopt legislative for other measures to establish as criminal offences when committed intentionally and without right, the causing of loss of property to another person by:

- a. any input, alteration, deletion or suppression of computer data
- b. any interference with the functioning of a computer system with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

Articles 9 of the Convention requires each Party to adopt legislative and other measures to establish as criminal offence, related to child pornography.

Articles 10 of the Convention requires to establish its criminal offences the infringement of copyright and related rights is defined under a party's laws.

For Articles 9 and 10 we have provided for these provisions under the current Cybercrime Act 2021 as well as our Copyright Act.

Article 11 of the Convention requires each Party to adopt legislative and other measures (as may be necessary) to establish as criminal offences (under its domestic law) when committed intentionally, aiding or abetting the commission of any of the offences established under (in accordance with) Articles 2 through 10 (of the present Convention) with intent that such offence be committed.

Article 12 of the Convention requires each Party to adopt such legislative and other measures to ensure that legal persons can be held liable for a criminal offence under or established under the Convention.

If we look at the Cybercrime Act, we are provided for this portion of the Convention in our penalty provisions where we have demarcated between natural persons and body corporates.

Article 13 of the Convention requires each Party to adopt legislative and other measures to ensure that criminal offences established under Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions.

Article 14 of the Convention provides the scope of the procedural measures for the purpose of specific criminal investigations or proceedings.

Article 15 of the Convention requires each Party to have in place safeguards and conditions to ensure the establishment, implementation and application of the powers and procedures under the Convention consistent to and in consideration of public interests, rights, responsibilities and legitimate interests of third Parties.

Article 16 of the Convention requires each Party to adopt legislative and other measures to empower competent authorities to order or obtain the expeditious preservation of specified computer data, including traffic data, where there are grounds to believe that the computer data is vulnerable to loss or modification.

Article 17 of the Convention requires each Party to adopt legislative and other measures to ensure expeditious preservation of traffic data that it is available and is sufficient enough to identify service providers and the path through which the communication was transmitted.

Article 18 of the Convention requires each Party to adopt legislative and other measures to empower competent authorities to order:

- a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
- b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

Article 19 of the Convention requires each Party to adopt legislative and other measures to empower competent authorities to search or access:

- a) a computer system or part thereof and computer data stored therein; and
- b) a computer-data storage medium in which computer data may be stored.

Articles 20 and 21 of the Convention require each Party to adopt legislative and other measures necessary in relation to serious offences to empower competent authorities to:

- a) collect or record through the application of technical means of that Party; and

- b) compel a service provider, within its technical capability to collect or record and to co-operate and assist competent authorities to collect or record content data and traffic data, relating respectively in real-time associated with specified communications in its territory transmitted by a computer system.

Article 22 of the Convention covers Jurisdiction where a Party must adopt legislative and other measures to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of the Convention. This we are provided for in the Cybercrime Act 2021.

Article 23 of the Convention outlines the General principles relating to international co-operation with relevant international instruments on international co-operation on criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data or for the collection of evidence in electronic form.

Article 24 provides for the principles relating to extradition. We currently have an Extradition Act in Fiji.

Article 25 of the Convention provides the general principles relating to mutual assistance which includes mutual assistance to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data or for the collection of evidence in electronic form of a criminal offence, the adoption of legislative and other measures necessary to carry out obligations under Articles 27 to 35. Form of requests by expedited means with the formal confirmations to follow.

Article 26 of the Convention allows a Party to forward information to another Party that it considers might assist the other Party in initiating or carrying out investigations or proceedings concerning criminal offences under the Convention or might lead to a request for cooperation by that Party.

Article 27 of the Convention outlines the procedures pertaining to mutual assistance requests in the absence of applicable international agreements including grounds for any postponement or refusal of requests.

Article 28 of the Convention applies where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between a requesting Party and the requested Parties for the supply of information on the condition that it is kept confidential or not, used for investigation other than those dated in the request.

Article 29 of the Convention provides for the expedited preservation of stored computer data by a State Party through request to another State Party for data located within the other State Party's territory or for which the requesting State is intending to submit a request for mutual assistance for the search or similar access, seizure or similar securing of disclosure of the data.

Article 30 of the Convention provides for the disclosure of a sufficient amount of traffic data where in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication. This, however may be withheld if the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence or that the execution of the request is likely to prejudice the sovereignty, security or other essential interest of the country.

Article 31 of the Convention allows a State Party to request another State Party to search or similarly access, seize or similarly secure and disclose data stored by means of a computer system located within the territory of the requested State Party including data that has been preserved pursuant to Article 29 - that is the expedited preservation of stored computer data.

Article 32 of the Convention allows a State Party without authorisation of another State Party to access publicly available stored computer data regardless of the geographical location of the data or to access and receive through a computer system in its territory, stored computer data located in another State, provided the lawful and voluntary consent of the person who has lawful authority to disclose the data through that computer system is obtained.

Articles 33 and 34 of the Convention require Parties to provide mutual assistance to each other in real time collection of traffic data associated with specific communications in their territory and real time collection or recording of content data with specified communications permitted under the applicable treaties and domestic laws.

Article 35 of the Convention requires each State, as highlighted by Madam APS, to designate a point of contact on a 24-hour basis, seven days a week to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data or for the collection of evidence in electronic form of the criminal offence.

Under Article 35 of the Convention, the State Party must ensure that trained, equipped personnel are available to facilitate the operation of this 24-hour network.

Article 36 of the Convention provides for the signing of the Convention by member States and Article 36 of the Convention also provides for the methods of being a Party to the Convention. That is ratification, acceptance or approval of the Convention where instruments must be deposited with the Secretary-General.

Article 37 of the Convention provides the process for accession to the Convention. That is the Committee of Members of the Council of Europe after obtaining unanimous consent of the Contracting States to the

Convention may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to the Convention as is the case for Fiji.

Article 38 of the Convention provides that any State may specify the territory or territories to which the Convention applies at the time of signature or depositing its instrument of ratification, acceptance, approval or accession. In the case of Fiji it is just for Fiji.

Article 39 of the Convention provides the purpose of the Convention which is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the European Convention on Extradition opened for signature in Paris. The European Convention on Mutual Assistance in Criminal Matters and the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters.

Article 40 of the Convention allows any State at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession to declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6, 9, 27 by written notification to the Secretary-General.

Article 41 of the Convention allows or provides for a Federal State to reserve the right to assume obligations under Chapter II of the Convention consistent with its fundamental principles governing the relationship between its central government and constituent States. This is not applicable to Fiji as we are not a Federal State.

Article 42 of the Convention allows any State at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, to declare that it avails itself of the reservation(s) provided for under specific Articles under the Convention Articles 4, 6, 9, 10, 11, 14, 22, 29 and 41.

Article 43 of the Convention allows a States Party that has made a reservation to withdraw such reservation either as a whole or partially by notifying the Secretary-General.

Article 44 of the Convention provides the means through which any Amendments to the Convention may be proposed by any Party again communicate to the Secretary-General to the member States, nonmember States and any State that has acceded to or has been invited to accede to the Convention.

Article 45 provides that the European Committee on Crime Problems (CDPC) must be kept informed regarding the interpretation and application of the Convention.

Article 46 requires Parties to undertake periodic consultations with a view to facilitate the effective use and implementation of the Convention, exchange of information on significant legal policy or technical

developments pertaining to cybercrime and the collection of evidence in electronic form; consideration of possible supplementation or amendment of the Convention.

Article 47 of the Convention allows the State Party to denounce the Convention by notification addressed to the Secretary-General.

Article 48 of the Convention requires the Secretary-General to notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of the Convention as well as any State which has acceded to, or has been invited to accede to, the Convention of any signature; the deposit of any instrument of ratification, acceptance, approval or accession; any declaration or reservation made or any other act, notification or communication relating to the Convention.

It essentially outlines the procedure that will take place if Fiji were to accede to the Convention. What happens then?

In a nutshell Mr. Chairman, Sir, that is the Convention. Thank you very much for this opportunity.

MS. T. BARAVILALA.- Thank you Ms. Glenys. Mr. Chairman, Sir, I would like to invite Ms. Catalina. Ms Catalina if you could please give your presentation. *Vinaka*.

MS. C. STROE.- Mr. Chairman, thank you very much for giving me the floor. Mr Chairman, Sir, and honourable Members of the Committee *Bula vinaka* again.

It is an honour to have the opportunity to address the Fiji Parliament Standing Committee on Foreign Affairs and Defence on behalf of the Cybercrime Programme Office of the Council of Europe (C-PROC).

As already mentioned, in this digital age we have witnessed that an open global free, peaceful and secure cyberspace is the foundation of prosperity, growth and security of our societies.

Digitalisation offers many empowering opportunities and development values to achieve a better future but it also comes hand in hand with serious potential vulnerabilities.

Cyberspace is certainly all about networks and we cannot address the security challenges it brings in a vacuum so isolate it.

Global cyber stability relies on the national ability of all countries to prevent and react to cyber incidents and investigate and prosecute cybercrime cases but also on their ability to effectively cooperate internationally with other States.

The Cybercrime Convention known also as the Budapest Convention is, as already mentioned, the only legally binding International Agreement on Cybercrime electronic evidence. As already presented by the representatives of the Solicitor-General, it creates Government standards for criminalising cybercrime offences, procedural powers to investigate cybercrime and any offence involving electronic evidence and tools for international cooperation that allow the parties to secure and access electronic evidence that may be located in other Parties.

Fiji was invited to accede to the Budapest Convention in December last year. Invitation to accede to the Convention sends an important signal about the countries' readiness to harmonise its internal laws with the international government standards in the serious fight against cybercrime and engaging in international cooperation to this end.

Being a party to the Convention allows the country to engage in international cooperation not only with respect to cybercrime but also with respect to any crime involving electronic evidence. And I will just give you one or may be two examples to contemplate that. Imagine a terrorist attack where your investigation teams need to preserve and receive data electronic evidence located in another State Party to the Budapest Convention.

Imagine the same scenario in a case of an ongoing kidnapping of a child. In terms of preserving and receiving electronic evidence on the case brought the investigation one party to the Convention can seek the cooperation of another State Party to the Convention where the data is located based on the provisions of the Convention. So you see how important and powerful this Convention on Cybercrime is.

Another important benefit as a Party to the Convention is that State Parties are members of the Cybercrime Convention Committee and in this capacity can share information and experience assessing the implementation of the Convention and interpret the Convention through guidance notes.

The Cybercrime Convention Committee has many guidance notes which are now published and if Fiji will be to finalise the accession process through the ratification will become full member with full rights of the Cybercrime Convention Committee being able to assess the implementation of the Convention and build together with the rest of the now 67 other member State parties to build further guidance notes.

As a Party Fiji will also be able to sign and ratify the other two additional Protocols to the Convention including the most recent one that was already mentioned by the Madam Acting Permanent Secretary (APS) that provides innovative tools and mechanisms for enhanced international cooperation. Likewise Fiji will be able to participate in the negotiation of the future revision of the Convention.

There are indications and here again, Madam Acting Permanent Secretary has already mentioned the private sector cooperation that are indications that private entities including giant Internet Service

Providers (ISPs) are most likely to voluntarily respond to requests of data if the request comes from an authority over the State party to the Budapest Convention.

Why is that? Because it is considered that these countries' State parties have a strong legal framework in place including safeguards to ensure that the right balance between the need to protect the citizens against any crime and the respect for fundamental rights and the rule of law.

In our experience we need to work together at all levels. This is why part of the commitment of the Council of Europe States that have been invited to accede or already are parties receive structured, tailored fit capacity building to strengthen their capacities on cybercrime and electronic evidence. And this is done through the Cybercrime Programme Office run from Bucharest Romania.

Currently we have 44 employees (staff) in the office. We have five ongoing projects for various regions, two of them are global and the one that I am managing is also a global one. We were able through Global Action on Cybercrime Extended (GLACY+) Project the Programme that I am running. We were able to add Fiji as a proactive country to the Project soon after it was invited to accede in less than six months afterwards and we are working together with the authorities from Fiji to make sure that any type of assistance and support on capacity building we are offering it is done in respect of the national contacts but also with the view of addressing the priorities and the needs that Fiji has in a particular moment in time in terms of strengthening the capacities of the criminal justice authorities in the fight against cybercrime and with respect through electronic evidence.

It was already mentioned by the Madam APS the free workshops took place in June this year for judges, prosecutors and law enforcement. This is just an example of the type of assistance that we can offer. We were called and told we would like to organize this workshop. We really need to see how criminal justice authorities are thinking through who are considering to implement the Cybercrime Act that we passed last year. We were there to do that together with the colleagues in Fiji and this is just the first step. We are going to continue because now we have the initial needs assessment done in June. We have a baseline from where to start from. We are in continuous contact with the colleagues in the Ministry of Communications to make sure that the priorities are properly addressed.

In the end I would like to just finish my short intervention by expressing the gratitude they have for offering this chance to present in front of the Committee and to reiterate the commitment of the Council of Europe and of the GLACY+ Project that works closely with the Fijian authorities to foster the positive work that lies ahead of us in our cooperation in this very challenging but very exciting field which is cybercrime and electronic evidence.

Thank you very much and I remain at your disposal for any type of questions you may have.

MS. T. BARAVILALA.- Thank you Mr. Chairman, that concludes our joint collective submission.

MR. CHAIRMAN.- Thank you Madam Acting Permanent Secretary, Madam Glenys and Madam Catalina for your very insightful contribution this morning. We will now open up for questions, I will ask the honourable Members if you do have any question, just raise your hand please.

HON. L.S. QEREQERETABUA.- Thank you Catalina, thank you ladies and gentlemen. What in your mind is the highest priority for online safety for Fiji at the moment? I know you have talked about your cross border attacks and so forth, but in your opinion, what is the most pertinent threat for Fijians?

MS. T. BARAVILALA.- Thank you for the question, Mr. Chairman through you, I will maybe just give a few opening remarks and I will open it up for my Directors as well because I know we have had a lot of discussions with various stakeholders in terms of the priorities. Yes, what we are talking about here is cyber security, cyber resilient efforts that are happening at the international level and really driving it back down which the question is in terms of nationally what we are doing. We have a lot of collaboration with the Online Safety Commission, Police and other stakeholders in terms of really identifying what is the threat landscape in Fiji.

Sir, to answer your question in terms of the priority that we see, and this is something that is evolving as we have more Fijians coming online, is really to ensure that there are responsible online users and they know how to navigate this online spaces which is also very new. I think a priority is looking at that and how can we better collaborate as various stakeholders so that there is an awareness in terms of what it means to be online. Very simply just looking at passwords and saying you know you would have people that would have their passwords written down, taped on to the laptop, very tangible sort of concrete things that can be done to increase internet safety and just safer cyber hygiene efforts. I think that is really does take everyone that has a platform, various stakeholders to come together so that we can increase that awareness in terms of what this means.

So even looking at multi-factor authentication which is something that really allows you for you to ensure that there is no one else that is trying to get into your account and so one of the things that we have been seeing as well is when you say things such as multifactor of application you sort of get a gaze in people's eyes because it is in a language that is not understood.

So really looking at various aspects, so for us it is not just the one thing but looking at behaviour and then really getting all the relevant stakeholders in the room to increase that awareness in terms of what does it mean to be safe online and I think that is the main priority so really unpacking or demystifying what cyber security is and bringing it down to the individuals so what does that mean for me? That means that I as a user should not have the same password for all of my accounts because for whatever reason one account gets hacked, we cannot go into your other accounts so you have a lot of people that would have the same account for all of their social media platforms and then you have someone that comes in and takes over that account. What it also means is ensuring that we are not writing up those passwords and putting that in.

Mr. Chairman and honourable Members, I am not sure if you had seen this, something was going on social media where it would say 'these are the 10 questions and you need to answer these 10 questions and send it to the next 10 people'. What is your favourite colour, what is the name of your favourite pet? There were these questions that were going online and you would see it in social media sort of *Facebook* and questions that you would have once you have answered the question, you give it on to 10 other people, they answer the question and it was get to know you a little bit more. What is your favourite colour? These sort of questions if you would look at your security questions, if you open a bank account or if you open an account it would ask you what is your childhood college or what is your favourite car model? It came out very innocently where you would be saying all these things but for most people that would actually be the password.

You have things that are guised as games and tells us a bit more about yourself and that refers to social engineering tactics that are being used, where they would know a little bit about you and then you would have someone that is just sitting somewhere massively going out doing web calls just trying to get all this information and then doing sort of attacks.

It is really an important component that we are looking at all of these on various funds and we really need to ensure that we have those safeguards and that is something that we are consistently having conversations on and how do we do that. We know that the Police have also a lot of outreaches that they do as well and they work very closely with Online Safety Commission to be able to get that message out. The other thing that we are also very mindful of is making sure that it is targeted sort of contempt, how you would communicate this with the senior community members would be different to how you would communicate it to students, and that is something that we also work very closely when we work with schools to also have those conversations as well. So I think that is just very briefly in terms of what we are looking at and I think this is something that we need to continuously look at because we do have evolving challenges that are coming so we always need to make sure that we are able to respond effectively but may be if I could have one of my Directors to be able to contribute.

MR. S. DEO.- Thank you, Acting PS, through you, Mr. Chairman, just to add on to what Acting PS was saying, and basically trying to put it into more a cyber incident concept I guess.

To start with, there are two kinds of people or businesses: those who know that they have been attacked and those that do not know that they have been attacked. I think the latter one is something that is quite dangerous and looking at the cyber hygiene practices like what the Acting PS mentioned, and in terms of how people are looking into increasing day-to-day cyber activities, be it individuals or be it someone who is working at a desk in an office or part of the internal network of the office or be it a large corporation.

Cyberattacks are not something that is new or no one is immune to cyber-attacks and I think in terms of, if you look at Fiji and through our discussions with other agencies such as the Cybercrime Unit of the Fiji Police Force as well as other agencies working in this place, I think some of the common things you will see is business e-mail compromise. Now how that happens? Some of it happens exactly like how Acting

PS mentioned, people know your e-mail because it is quite public to guess your password or to try and reset your password they use the social engineering techniques to get your favourite colours, what school you went to or what is the name of your first child, et cetera. They go and do a bit of reinforce, trial and error method and they are able to get through. Once they are into your business e-mails then they can do a lot of financial damage to a company, and this is largely prevalent in the financial sector and the health care sector, if you look at that globally.

The other thing that we see quite common in Fiji is Phishing Attacks, which comes in multiple flavours and I think this is how we traditionally fish, except it is the phishing with a 'p'- p-h-i-s-h-i-n-g. So you cast a very wider debt and it is either e-mail campaign targeting particular individuals with the link to click or it opens up a form and you submit certain details or it is called Smishing (SMS Phishing), there is Vishing voice calls, then there is Spear Phishing. You know somebody who is a very important individual in an organisation, you try and get information from that person, sort of directly targeting that person to get information or access to internal networks. If you have seen recently, some of our mobile wallet, money service providers have put out certain advisories that if you get a call or an SMS asking for your one time password do not respond to it. Those are some types of phishing that is happening currently in Fiji and you will see how advisories are being put out.

We have seen ransomware attacks as well occurring globally, and I think it is something that we cannot localise to Fiji because largely it is borderless, a non-kinetic attack on a particular agency or an organisation which the cyber makes it borderless.

Then we have seen Denial of Service, whereby much traffic is put to your server that suddenly with the legitimate connections are not able to go through. Those are some examples of cyber incidents that do happen in Fiji.

MR. CHAIRMAN.- Madam Catalina, would you wish to comment on that question before we go to the next one.

MS. C. STROE.- Thank you very much. May be just to mention that in my experience prevention and combating are the two sides of the same coin and an indeed very valuable and important point mentioned by Madam Acting PS and her Director and just to mention that from our side what we are trying to do with the capacity building projects including GLACY+ that I am running is to make sure that we prepare the criminal justice authorities and the law enforcement authorities to make sure that the part on combatting is also prepared in case the prevention does not, 100 percent, work. Both sides are very well-connected, when one is not working the other one is not working also because if the citizens are not trusting the criminal justice authorities they will not report. If they will not report, there is nothing to investigate and the crimes perpetuate. So we need to make sure that both sides of the coin work perfectly together. Thank you very much, only that from my side.

MR. CHAIRMAN.- Thank you, Madam Catalina. Honourable Peceli, you have a question.

HON. P.W. VOSANIBOLA.- Thank you, Chair, through you, just a question: What backup systems do we have if there is a cyber-attack on government information, data and other very important information? Thank you.

MS. T. BARAVILALA.- Thank you for the question, Mr. Chair, through you, this is what I had mentioned earlier in terms of, there is a lot of layers or safeguards that really need to be put in place to ensure that we are protected and that is one of those components as well. So with regards to government sort of infrastructure, we do have a tier three data centre that is available so it is critically important and Director had also mentioned this earlier - the two types of people but also the attacks are happening. It is not that attacks are not happening, attacks are happening across the board and we see this but what is critically important is ensuring that we have really close collaboration with development partners, with partners such as the Council of Europe but also the security of who has the technical expertise so your various firewalls, the various data protection sort of mechanisms that we have in place to ensure that we are resilient when it comes to cybersecurity.

The other thing I think on the other side that is quite important as well is, not just in terms of, you know as defence mechanisms, which we have in place but also when you look at the software that is being developed by government, particularly you know that is done under the digital government initiative. Every software development that is done at the very beginning we are thinking about privacy preserving measures and we are also thinking about and incorporating data protection measures as well. So these are things that even when we are deploying our services, that is at the core of what we are thinking about and it comes back to our mandate which is ensuring that Fijians are safe, as we connect more Fijians we are making sure that they are safe online. So thank you for the question. That is something that, you know, is of utmost importance to us and something that we are continuously monitoring and ensuring that we have that covered. I am not sure if I have further comments from Directors on that question.

HON. P.W. VOSANIBOLA.- Thank you, Mr. Chair. Just through you since we are having this technology, do we still rely on manual and keeping up of data(s) or are we phasing out from those files et cetera.

MS. T. BARAVILALA.- Thank you for the question. Mr. Chair, through you in terms of the data that we do have, you know it is not a matter of phasing out from manual files and forms, it depends on the type of data that we are talking about, so if we were to talk about government data, there are certain components of that but it is not a direct switch.

We also need to be mindful in terms of why we are doing what we are doing and at the same time ensuring that in whatever form it is at, whether it is manual or digital, that we have those protection measures in place so I hope that answers your question honourable Member.

HON. S. ADIMAITOGA.- Thank you for your elaboration this morning and very empowering too. I would like to ask: which nature of crime is not covered by Budapest Convention, because the Convention itself demands harmonization of social legislation?

MS. T. BARAVILALA.- Thank you for the question. Mr. Chairman, Sir, it is a very interesting question because the Convention deals with Cybercrime and any crime that has electronic evidence. Right now if we were to define what a computer is, a few years ago a computer is the monitor, the screen and your keyboard. Today this can be a computer and also smart devices or the smart watches. I would be hardpressed to find any particular crime because it would be any crime that deals with electronic evidence so an SMS message, a text message, an email, across the board if it does not have those elements then I would assume that it would not apply but I would be hard-pressed to find any sort of crime that does not have an electronic evidence component to it and I would also invite Ms. Glenys from SG's office.

MS. G. ANDREWS.- Under the Convention on Article 1, the definition of "computer system" is provided for and it means any device or a group of interconnected or related devices, one or more of which, pursuant to a programme performs an automatic processing of data. So at a minimum or as a basis, the definition of a "computer system" is provided for under the Article and when we look at this specific provisions that the Convention addresses with respect to substantive criminal law, it talks about the use of a computer system which as Ms. Baravilala has elaborated on, expands over a variety of devices - anything that falls within that definition.

I would not go too much into the technical bits, I will leave that to the experts but it is basically the use of a computer system, using that to commit specific criminal offences or specific offences that are criminal in nature but with the use of a device or a system that works within that definition provided for under the Convention. We have factored that also in to the Cybercrime Act 2021, for your information Madam.

MR. CHAIRMAN.- I have a question, just very brief probably a yes or a no from Madam Catalina: Your C-PROC office in Europe, does that operate 24-7?

MS. C. STROE.- Thank you very much, Mr. Chairman for the question. It may seem now that I am online that we operate 24-7, like the 24-7 network but our office is only doing capacity building. That means we offer technical assistance to countries who would like for example on legislation or to countries as Fiji for us now on structured tailored-fit capacity building. This is different from the 24-7 network which operates on presumption of 24 hours 7 days per week. I do hope that I have answered your question but now lately we are available 24-7 indeed also but only on capacity building.

MR. CHAIRMAN.- Thank you Madam Catalina. A question for the presenters: I am an old school but perhaps if I could just ask you why did we pass the Bill (which is now an Act of 2021) and we are going through the process now of acceding. Can you give me some ground behind that, please?

MS. T. BARAVILALA.- Mr. Chair, may be I will start: The provisions under the Convention in terms of any State that is wanting to accede to the Budapest Convention it does outline that you either commit to taking the necessary steps to domesticate the provisions of the Articles. What we actually did was we focussed on getting the law first, getting that passed and we then express an interest. So may be Ms. Catalina Stroe might be able to provide a bit of insight from her side.

Mr. Chair what I have seen because I have been attending a few of the meetings is, you would have a few countries that would say 'Alright I commit to doing what needs to be done in the various provisions' and then once accession they would then do that.

Fiji has been very committed because we understand the need for this and we understand why we need to accede or go through the process.

So as I had mentioned earlier in other sort of treaties we could just accede or given you know be able to take those steps very quickly. We have to sort of show that we would do that not only did we do that we actually went ahead and got the law done.

So that is why I think it was just the couple of months. It then had to go through the process of all of the current member States actually having a consensus that, yes, Fiji be invited.

So all of these concrete steps that we have been taking to show that this is something that we need to do and very strong in our commitment that has actually resulted in us receiving that invitation on the 8<sup>th</sup> of December, 2021.

There is a certain time that is given and that is also in the Convention whereby you can accede but what we are saying is, we are at a point in time now where cyber-attacks are happening left, right and centre. We do not have the luxury of time and we also you know our law enforcement agencies require these various levels of cooperation to be able to effectively combat cybercrime.

We have seen a lot of cases in a lot of countries and member States being in state of emergencies because of the sophistication of the crimes that are coming. And for us this is us future-proofing the work that we are doing in terms of the digitalisation and all of the investments that we are doing we also need to ensure on the other side that we are protecting everyone.

So if I understand your question correctly, Mr. Chair, the reason why we did the law first and we then did the accession is so that we can show our strong commitment that this is something that you know we view as a priority and that has been taken as such as well.

I have been in a lot of meetings with the Council of Europe where they are very happy and also the fact that we have been able to do so much in such a short period of time and I think it is just because all of the stakeholders have a consensus that, yes, this is important and we need to do this. So that is why we took that approach. It is faster and within a short amount of time we were able to get the invitation and we are working hard now which is why we are reiterating our support in terms of that Fiji accede to it because it is in our best interest to do so.

MR. CHAIRPERSON.- The reason why I asked that and perhaps Ms. Andrews may wish to comment or not but it is very similar to the Intellectual Property Rights Bill that we amended about two years ago I think in 2020. Yes, that is why I touched on that but thank you for the answers.

Honourable Members, any further question, no.

Alright at this juncture I wish to sincerely thank you all and you in particular Ms. Catalina having tuned-in in some ugly hour of the world this day and thank you all once again for that.

On behalf of the Committee we wish you a blessed day and please keep safe. With those few words if you have any parting comments the floor is yours, thank you.

MS. C. STROE.- Thank you very much. I just want to say how grateful I am to be able to speak in front of you and to congratulate Fiji for the approval of the law. It was as Madam APS said “great achievement”. We proudly worked together with the counterparts in Fiji on the draft law and we were very happy when it was approved and later on it was a great achievement to us all that Fiji was invited and we are looking forward to the finalisation of the accession process and we promise you we are going to be by your side the rest of the way. Thank you very much for having me.

MS. T. BARAVILALA.- Thank you, Mr. Chair. Also may be as concluding remarks from our side: if there are any other questions that the Committee may have for us I understand that there is further consultations that are taking place. We are very happy to provide our clarification, answers or responses to those questions but thank you once again for the opportunity to be able to submit our contributions and interventions regarding this motion.

MR. CHAIRPERSON.- Thank you vinaka vakalevu.

The Committee adjourned at 11.11 a.m.

**VERBATIM REPORT OF THE MEETING OF THE STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE HELD IN THE BIG COMMITTEE ROOM (EAST WING), PARLIAMENT PRECINCTS, GOVERNMENT BUILDINGS, ON TUESDAY, 27<sup>TH</sup> SEPTEMBER, 2022 AT 9.30 A.M.**

**Interviewee/Submittee:** - University of the South Pacific

**In Attendance:**

1) Professor Jito Vanualailai - Deputy Vice-Chancellor (Education)

---

MR CHAIRMAN.- Honourable Members, members of the public, the secretariat, Hansard, ladies and gentlemen; a very good morning to you all. It is a pleasure to welcome everyone, especially the viewers that are watching these proceedings.

For your information, pursuant to Standing Order 111 of the Standing Orders of Parliament, all Committee meetings are to be open to the public. Therefore, please note that this submission is open to the public and media, and is also being streamed live on Parliament's website and social media online platforms, and the Parliament channel on the *Walesi* platform. For any sensitive information concerning the matter before us this morning that cannot be disclosed in public, this can be provided to the Committee, either in private or in writing. Please be advised that pursuant to Standing Order 111(2), there are only a few specific circumstances that allow for nondisclosure and these include:-

1. National security matters;
2. Third party confidential information;
3. Personnel or human resource matters; and
4. Committee deliberation and development of Committee recommendations on reports.

I wish to remind honourable Members and our guests, that all questions are to be asked and addressed through the Chair. This is a parliamentary meeting and all information gathered is covered under the Parliamentary Powers and Privileges Act. Please, bear in mind that we do not condone slander or libel of any sort, and any information brought before this Committee should be based on facts.

In terms of the protocol of this Committee meeting, please minimise the usage of mobile phones and all mobile phones are to be on silent mode while the meeting is in progress. Allow me now to introduce the Members of my Committee.

*(Introduction of Committee Members and Staff)*

MR. CHAIRMAN.- Unfortunately, not with us today is my Deputy Chairman, honourable Dr. Salik Govind who is on bereavement leave overseas.

Today, the Committee will be hearing a submission on the Convention on Cybercrime otherwise known as the Budapest Convention. For the purpose of the viewers that are joining us this morning, allow me to give a brief explanation on the Treaty.

The Convention on Cybercrime (also known as the Budapest Convention) provides a comprehensive and coherent framework on cybercrime offences and electronic evidence. It serves as a guideline for any State developing comprehensive national legislation against cybercrime and as a framework for international cooperation amongst States' parties.

To-date the Convention has 67 members which includes Australia and Tonga from the South Pacific Region. Pursuant to Article 37 of the Convention any other State such as Fiji can become a party by accession if the State is prepared to implement the provisions of the Convention and upon invitation to accede to the Convention after consultation and approval of Parties. With the extreme effects of global cyber threats and attacks on critical sectors such as Finance, ICT, Energy, Water, Emergency Services, Public Safety, health, public services, aviation and e-government infrastructure becoming a party to the Convention will enhance Fiji's ability to combat cybercrime with international support and assistance, particularly in relation to continued capacity building to better equip Fiji's criminal justice authorities including the judiciary, prosecution and law enforcement agencies.

Ladies and gentlemen, before us this morning we have the Deputy Vice-Chancellor (Education), Professor Jito Vanualailai. The floor is yours Sir.

PROF. J. VANUALAILAI.- Thank you so much honourable O'Connor, the Chairman of the Standing Committee on Foreign Affairs and Defence, the honourable and esteemed Members of the Committee, honourable Adimaitoga, honourable Qereqeretabua, honourable Vosanibola and the esteemed Members of the Committee.

Foremost, I would like to thank you for inviting the University of the South Pacific (USP) to submit its comments on the Budapest Convention. The university as you know, is a tertiary institution and its main role is to produce and disseminate knowledge, therefore it is looking at the Convention from two perspectives:

- i) If it is ratified by Fiji whether we have the local capacity and capability to support Fiji; and
- ii) That our ability to fight cybercrime at the forefront of technology in the sense that we should have the skills and the knowledge to fight cybercrime, and whether the university could convince the

Committee that it has the capacity or the capability to train our human resources in the future to support the Convention.

In general, the university believes that the Budapest Convention provides the necessary framework for international cooperation in fighting cybercrime. Therefore, USP supports Fiji in ratifying the Budapest Convention if Fiji wishes to do so. As I mentioned, USP is looking at the Convention from two perspectives with respect to fighting cybercrimes. Firstly, USP is systematically developing human resources in cybersecurity and secondly, USP is helping ICT enterprise practitioners in ensuring cybercrime free digital networks.

In human resources development, USP offers a number of courses in its undergraduate programmes and in its post graduate programmes in both areas of cybercrime and cybersecurity. Therefore, through its various courses in the different programmes, I can assure you that USP is empowering the future workforce with the right knowledge and resources, and is helping create a well-equipped and trained society to fight cybercrime through our academic programmes. That is the first assurance that USP can support Fiji if Fiji wishes to ratify the Budapest Convention - through the training of appropriate human resources in Fiji.

Also USP has the capability to support the private sector. Indeed in terms of ICT services capability, USP stands ready to continue to support the Fiji Government and indeed the regional governments in the adoption of the Budapest Convention against Cybercrime. As an example to this, USP's internet presence in the global research and education network is brokered through the Australian Academic and Research Network (AARNet) which essentially compels USP to comply with the Budapest Convention given that Australia as I mentioned, Mr. Chairman, is already a signatory. Therefore in summary, when USP considered the Convention it did so from the perspective of whether we could help the Fiji Government (if it wishes) to ratify the Convention; whether it could support the provision of trained human resources; and whether also it could support the private sector in understanding the implications of cybercrime and cyber security.

I would like to show you, as I mentioned, that USP stands ready to help and it has the resources to train future human resources in Fiji through its various academic programmes. Also as I mentioned it has experienced through the Australian Academic and Research Network (AAR-Net) with respect to understanding cyber security. With this submission from USP, I wish you all the best, Mr. Chairman and the honourable Committee Members in your deliberations.

MR. CHAIRMAN.- Thank you Professor Vanualailai for your and the university's insights on this Convention. Honourable Members, floor is open for questions.

HON. S. ADIMAITOGA.- Mr. Chairman, through you, can you explain the network services which is responsible of the design and implementations of the data network in the new construction as well as the renovations to the existing facilities?

PROF. J. VANUALAILAI.- If I understand your question clearly, honourable Adimaitoga, are you looking at the physical construction of a network and how the issue of cyber security is concerned with the data in the network?

Mr. Chairman, I can only share my experience with respect to the university. As you know, honourable Adimaitoga, we have a very comprehensive digital network. It is called the USP Network which digitally connects 12 member countries, not only through the satellite but also the undersea cable which is connected to the AAR-Net - the network that I was talking about.

Sir, in order for USP to ensure that the issues and conditions of cyber security are met and that the conditions of the Budapest Conventions are met, we aligned ourselves to AAR-Net, so indeed our network is a subset of the AAR-Net network. As I mentioned, Australia is already a member of the Budapest Convention, we are therefore compliant to the conditions of the Convention. As you see, honourable Adimaitoga all the Budapest Convention Articles are the conditions that we are adhering to and it is necessary that those Articles be adhered to if we decide to construct a digital network. Indeed it is a framework before we physically construct a network - it is a framework that needs to be adhered to, to ensure that if a cybercrime is being committed the network should be able to detect this and be able to allow the enforcers to enforce the Articles in the Budapest Convention.

HON. P.W. VOSANIBULA.- Mr. Chairman, through you, Professor Vanualailai just a simple question. Within your institution so far, did you have any incidents of cyber-attacks on your networks, and if that happened what remedy action was taken?

PROF. J. VANUALAILAI.- Mr. Chairman, let me tell you that we are being attacked daily from various parts of the world. The attack is basically trying to penetrate our system through various means in order to get data from the University. I think we are fortunate that we have built our experience over the last 30 years with the help of our stakeholders and the Fijian, Australian and New Zealand Governments to build a secure system. If I were to take you honourable Members to the University, we can go into the war room, you can see on a big screen where the attacks are coming from, it is just incredible. When we have big meetings like the Pacific Island Forum Leaders Meeting, the attacks come in left, right and centre because once they penetrate one of our systems in Fiji, they can penetrate elsewhere. Yes, we are being attacked daily, but let me assure you that we have a good team at the USP and we have counter measures against these attacks. But once in a while, it seeps through, and I think maybe it was three or five years ago where an attack succeeded and our system was down for a while. They were able to penetrate our computers and so forth, but we learnt from that and let me tell you that the attack continues on a daily basis.

HON. S. ADIMAITOGA.- Mr. Chairman, due to your explanation this morning regarding cyber security at USP in computing systems that relies heavily on the use of codes. Does it ensure confidentiality and secrecy of protected information - can you elaborate further on that?

PROF. J. VANUALAILAI.- Mr. Chairman, definitely - in a computer secure system (and that is one good thing about the Convention), it protects individual rights and there are different level of access. At the top level of course, you have those computer programmers who can access the security of the system, but cannot actually access an individual private account because of our human right as well. That could also, of course, open up the possibility of misuse by those holding a private account - that is where the whole concept of the Convention is about - how do we catch those who are abusing their private accounts. As I have mentioned, those who are delivering a network service, can only deliver it at the top level where they provide you the services, but they have no authority to go down to your private account, because again, it is the concept of confidentiality and the issue of human rights as well.

If an individual is abusing the system, there are other ways to capture that and the Convention lists down some of those, for example, some of those could be an unusual access to several sites which may be forbidden. It could be sites that deal with hacking for example and the system can capture the frequency of accessibility to certain sites, maybe child pornography for example, and then it gives off a warning that there are several activities being carried out. It could be money laundering for example, and therefore there is a need to look into it. If there is a need to look into it, that is where the Convention then gives the right to the government to do certain things like, for example, the police could come in and take your equipment to check what is happening inside. But in general, the good thing about the Convention is that it also prioritises the human rights and as long as we do the right thing, it is lawful - what we are doing is lawful - then your privacy is protected. Yes. Thank you. *Vinaka.*

HON. L.S. QEREQERETABUA.- Thank you, Chair. Through you I just wanted to ask the Professor – nothing to do with the Convention. Just great to hear that you have got a great team in your war room. I just wanted to know – are they all home-grown?

PROF. J. VANUALAILAI.- Thank you, honourable Qereqeretabua. I am sitting down here and I am so proud as a Fijian, as a Fiji citizen to say that not only are they home-grown, they are our kai Viti, they are together with us, they are Fiji citizens - home-grown and they are trained in Fiji. All of them are really proud Fijians and they are protecting the University to the best of their ability and they are very skilled workers. We have got great people like Josefa Ratuva whose father is a professor and they are definitely home-grown and I am proud to be part of the team. *Vinaka va'levu.*

MR. CHAIRMAN.- Thank you, Professor Vanualailai. Any other questions, Members?

Sir, I take this opportunity to say thank you again for availing yourself and should the Committee need to have further dialogue with your good self or have questions, that you will avail yourself at a later time. I also take this opportunity to be able to wish you well and your team particularly through this post-COVID-19 era and hopefully we can move forward together. Thank you.

PROF. J. VANUALAILAI.- Thank you, Chair, honourable O'Connor for this opportunity and thank you esteemed Members of the Committee. All the best in your work. *Vinaka.*

The Committee adjourned at 9.54 a.m.

**Interviewee/Submittee:** Fiji Women's Rights Movement (FWRM)

**In Attendance:**

- |    |                   |   |   |
|----|-------------------|---|---|
| 1) | Ms Nalini Singh   | - | Executive Director                                    |
| 2) | Ms. Laia Bulatale | - | Team Leader Gender and Transitional Justice Programme |
| 3) | Ms. Bernice Lata  | - | Legal Rights Officer                                  |
- 

MR. CHAIRMAN.- Ladies and gentlemen before us this morning we have the Fiji Women's Rights Movement and I take this opportunity to request the Executive Director, Ms. Nalini Singh to introduce her team and proceed with their submission after which there will be a question and answer session. Thank you madam - the floor is yours.

MS. N. SINGH.- Thank you Mr. Chairman, Sir, for the kind words of introduction. My team today comprises of Ms. Laia Bulatale who is the Team Leader of our Gender and Transitional Justice Programme and I have here with me as well Ms Bernice Lata who is our Legal Rights Officer. I will present to you our submission and will be glad to take in any question that you and the Committee might have.

By way of introduction, the Fiji Women's Rights Movement (FWRM) was established in 1986 and we are a multi-ethnic and multi-cultural, non-governmental organisation committed to removing all forms of discrimination against women, through institutional reforms and attitudinal change through targeted research and advocacy. Our now being a feminist organisation, FWRM uses feminist analysis as the basis for this submission to address gender inequality.

Global developments in information and communication technologies has meant the increasing number of online users, sharing of personal information online and the availability of surveillance systems and mass data collection capabilities from both large companies and government. The right to privacy from increased government surveillance and mass-government data collection in Fiji remains an unexplored territory. In 2015 allegations from neighbouring countries spying on Fiji surfaced in mainstream media which sparked a national debate on privacy laws and protection of Pacific Island countries from international surveillance.

The impacts of such invasion of privacy on women, children and vulnerability remains unclear and undocumented. The FWRM takes this opportunity to submit here in our analysis and recommendation in response to the State's intention to adopt and ratify the Convention on Cybercrime otherwise known as the Budapest Convention.

First, the guiding principle in Cybercrime Convention must be adopted into law such as the recent Cybercrime Act of 2021 in particular the following;

1. Mindful of the need to ensure a proper balance between the interest of law enforcement and respectful fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedom;
2. The 1966 United Nations International Covenant on Civil and Political Rights (UNICCPR) and other applicable international human rights treaties which reaffirm the right of everyone to hold opinions without interference. As well as the right to freedom of expression including freedom to seek, receive and impart information and ideas of all kinds regardless of frontiers and the rights concerning the respect for privacy.

There needs to be a detailed list of guiding considerations outlined in the local law corresponding to the Cybercrime Act 2021, pursuant to this new Convention where the State is intending to accede too. In the absence of which there is a risk of misinterpretation of the law when being applied and carries a danger of violating the human rights of citizens, including women human rights defenders who often bear the brunt of draconian laws which seek to suppress the full exercise of human rights including the freedom to freely express opinions and to hold the State accountable for its actions.

The rights to privacy of Fijian women and girls from mass government surveillance and data collection more so in the context of COVID-19 - must be a priority. As articulated in the introductory section of this submission the right to privacy from government surveillance and mass data collection in Fiji is an unexplored territory till now. The role of government during a national emergency, disaster or a pandemic like COVID-19 is to protect the rights and freedoms of its citizens as enshrined under the Constitution.

The rationale of increasing government surveillance and mass data collection will be unlawful and intrusive on women and girls right to privacy unless the government follows strict criteria that is transparent. The second point is acknowledging the gendered nature of cybercrimes. The Cybercrime Convention is intended to assist States in combating cybercrime both locally and across borders. Fiji's Cybercrime Act 2021 also intends to do the same. FWRM submits that the issue of cybercrime should not be looked at from a gender neutral perspective but rather should be gender analysed so that we can know exactly how cybercrime is committed and against whom, by who? The victim and the perpetrator profiles are very important to gather. With 64 percent of Fijian women having ever experienced physical, sexual gender based violence from their intimate partners, we humbly submit that this will most likely crossover to cyberspace whereby we see crimes against women and girls being perpetrated online.

If we had published sex and age disaggregated data from Fiji's Online Safety Commission we will actually see how many women and girls have been subjected to online abuse in the form of gender-based violence. Dissecting how cybercrime occurs, can assist the State in providing gender responsive prevention strategies to make our girls and women safe online. In the last annual report published on their website for the year 2017-2018 the Fiji Police Force, CID, Cybercrime Unit recorded eight cases annually.

For the offence of publication of obscene materials, six cases were reported. There is no sex or age disaggregated data for these registered complaints. The use of online spaces to perpetuate intimate partner violence, for example, in Domestic Violence Restraining Order (DVRO) proceedings, is not captured. But we submit that women who have regular access to online spaces are more vulnerable to being exposed to violence online. The police data is not corresponding with the reality of women in Fiji.

In the world of work, at least for female journalists in Fiji, cyberspace is not a safe space at all. This was a significant finding in the collaborative case study on the prevalence and impact of sexual harassment on female journalists in Fiji, carried out by the University of the South Pacific and the Fiji Women's Rights Movement in March of this year. It showed that 83 percent of the respondents had experienced sexual harassment via online platforms including social media. This shows that crimes against women and girls are being committed online and thus need a closer look by the State to make online spaces safe for everyone. Acceding to the Cybercrime Convention will help with this, provided that there is an urgency by the State to make online spaces safer for all women and girls in all our diversities.

In conclusion, FWRM welcomes the States intention to accede to international Conventions such as the Cybercrime Convention, but it must do so in the spirit of also welcoming its guiding principles which will ensure greater accountability and restraint on powers of the State to unjustifiably encroach upon the rights of the citizens including women human rights offenders. The State must also prioritise the safety of women and girls in cyberspace and must take all necessary steps to prevent violence against all women and girls in their online space.

HON. S. ADIMAITOGA.- Through you, Mr. Chair, I believe that human rights should not be politicised - impartiality and objectivity were crucial to promoting the development of the International Human Rights. Is the Council focused on creating a conducive environment under which Fiji was encouraged to fulfil their human rights operations?

MS. N. SINGH.- Through you, Mr. Chair, I will ask my colleague to respond.

MS. L. BULATALE.- Fiji is signatory to different human rights mechanisms and frameworks, one of which FWRM monitors closely is CEDAW. There are other different conventions with human rights principles and frameworks where the State parties are obliged to carry out, despite whichever government or political party is in power. I think that if we go by that premise irrespective of the political context that we are in, I think that the principles of human rights in all those convention will inform the way in which laws are domesticated in Fiji. I hope that I have answered your question.

HON. S. ADIMAITOGA.- Through you Mr. Chairman, further to that, were there any interactive dialogue on promoting the Budapest Convention?

MS. L. BULATALE.- In terms of FWRM's work and the work that we do in this area, we go by our constituencies, so whatever evidence-based information that we are presenting to the Council this morning is from women and girls themselves - it represents the voices of women. In terms of making sure that our submission is consultative, we have made sure that the data that we are presenting are from women, in terms of making sure that people understand - the women understand what we are representing, it is already captured.

Maybe I could just add, I think in Fiji in terms of understanding what the Convention is, understanding what it entails, I think it is more than words, so in terms of the work that we are doing, that is something that is constantly ongoing.

MS N. SINGH.- Thank you Mr. Chairman. I think the Committee Member was referring to the Human Rights Council if I am not mistaken. I think my colleague has explained the Council and the work it does in setting up certain treaties and conventions - that work is contributed to by member States in a nonpartisan way. So that is without any political leanings and the work that we then bring into holding the States accountable if they are party to that convention, is also done with that lens. It is in terms of accountability and not looking at it through a political lens.

As my colleague said, despite whichever and whoever is in government, the international conventions signed upon do take precedence and they are the overarching international law that we abide by.

HON. L.S. QEREQERETABUA.- Thank you Mr. Chairman, through you, I noticed that you mentioned that disaggregated data is not easily available to you? Has that been a matter of practice or is there a reason why that is not made available?

MS. N. SINGH.- Mr. Chairman, thank you for the question. Having data desegregated by the most basic elements of desegregation which is by sex – yes, for a period of time we have not been able to get that because the administrative data by different institutions are not being shared in that way. Even with the police annual report that we looked at, in some of these categories the data is not desegregated.

Why we are calling for desegregated data (at least on the basic element of desegregation which is sex) is exactly what he have said. We do need to know the profiles who the victims are and who the survivors are because then, this will enable the institutions that are meant to be responding to these issues being brought up, be brought up in an appropriate way. We cannot have laws and the subsequent elements in it being gender neutral because we cannot have the same type of response to a man and woman regardless of where they are. You have to have an understanding of how a woman would have suffered verses how a man would have suffered in context with what resources and enabling environment is available to the man, and available to the woman to report and get justice from the formal justice sector. That is why, it is vitally important for our laws and policies to ensure that it is not gender neutral and we must be able to get disaggregated data at least on the basis of sex, in the institutions that are linked to providing the response.

HON. P.W. VOSANIBOLA.-Mr. Chairman, through you, a question in regards to your submission on your first issue of concern, that there needs to be a detailed list of guiding principles and considerations outlined in the law - it refers to the Cybercrime Act 2021. Sir, I just need an elaboration on what it continues to say that “in the absence of which there is a risk of misinterpretation of the law when being applied”. Can you just elaborate further on that?

MS. N. SINGH.- Thank you, Mr. Chairman, I will ask my colleague Ms. Lata to respond.

MS. B. LATA.- Thank you for the question. When we were preparing the submissions for today, we did our research on the piece of law that was enacted last year which is the Cybercrime Act. I believe when the Cybercrime Act was being consulted upon we had made submissions at that time as well. We saw that there were similar provisions in the Cybercrime Act (the local law) which was corresponding to the Budapest Convention.

At that time, we had submitted that the principles part of the Convention should also be codified in the local law because it can have an international Convention that the States signs on. But if you do not have the safeguards in check - the guiding principles to limit the powers of the State in encroaching upon the rights of the citizens, then that is the risk that we are alluding to. There is a danger of overreach of powers of the State and also to not have human rights defenders being able to do their work in holding the State accountable - that is what we referred to. We need the principles that are part of this Convention that the State is intending to accede to, in consideration of the guiding principles, if that could also be codified into local law to have more impact. There is formal recognition in the law and that would be the basis by which the State can utilise the law to actually implement the Cybercrime Act.

HON. P.W. VOSANIBOLA.- Mr. Chairman, in addition to that question, that was during the consultation period. So the Bill has been enacted, does it have some of the regarding principles or your concerns?

MS. B. LATA.- I stand to be corrected, Mr. Chairman, but when we read upon the Cybercrime Act, in the beginning we could not find principles of interpretation. I stand to be corrected on that.

MR. CHAIRMAN.- Honourable Members, are there any further questions? No? thank you for that. On that note, the Executive Director – Ms. Singh; thank you and your team for your very informative submission on your thoughts and we take this opportunity to thank you once again. Should we have any other questions or queries, we do hope that you will avail yourself at a time of your convenience. With those few words, thank you once again and wish you all the best. Thank you.

The Committee adjourned at 11.24 a.m.

**Interviewee/Submittee:** Fiji Law Society

MR. CHAIRMAN.- Ladies and gentlemen, before us this morning we have the staff of the Fiji Law Society, and I take this opportunity now to invite Madam Mele Rakai, the team leader, to introduce your staff, and proceed with your submission, after which, there would be a question and answer time.

MS. M. RAKAI.- Mr. Chairman, the Standing Committee on Foreign Affairs and Defence and honourable Members, it is a privilege to submit to you under Convention of Cybercrime, known as the Budapest Convention. On behalf of the Fiji Law Society, its President - Mr. William Clarke, its Council and members, with me is Ms. Lilian Mausio - Fiji National University who is here in her capacity as an individual, Ms. Lavenia Bogitini of SLS Legal and Mr. Robakeibau Nayacalevu of Fiji Law Society secretariat. I am from Sherani & Company but we are all members of the FLS and it is a great privilege to submit to you.

I do not wish to bore you with our submission this morning as I am sure you have been listening to many committees that have been submitting to you. Ultimately, it is this Committee in Parliament which is the arm of legislature which will have the final say. Our role is simply to assist you, Mr. Chairman and the Committee, on whether this proposed Convention will benefit the country. While 67 countries are parties to this Convention, Fiji is part of the 15 countries, including New Zealand and Vanuatu who have been invited to accede this law. However, in order for Fiji to implement the provisions, as Mr. Chairman has mentioned, Fiji would need the rest of the parties to agree to be part of the Convention.

If I may now proceed to dealing with the Articles. What we have done is, we have divided the Articles amongst us, so I will be the first speaker, the second speaker will be Ms. Mausio and then Ms. Bogitini. We have decided only to talk on the pertinent Articles and we have the copy of our written submissions which we have provided. We can also have that submitted electronically for the Committee to read.

If I may go on to Article 1. The definitions in Article 1 of the Budapest Convention, when we look at it, it deals with the definition of computer systems, computer data, service provider and traffic data. If you look at those provisions, they are very similar to the Cybercrimes Act 2021, which has already commenced in Fiji, in February of last year. Now this Act had repealed Part 17 of the Crimes Act, Division 6 which had dealt with computer offences, and had inserted consequential amendments.

Our submission is that because they are already part of the Cybercrime Act, there is no need to accede to this provision because it is already there. Our suggestion though is that we could include a little bit more of the definitions that we see are missing and our second speaker (Ms. Mausio) will deal with the need to have a definition of content data - that is missing.

We also rely on the earlier submissions that were made by the Fiji Law Society which had dealt extensively with its proposals on what we thought should have been included. The other provision that was dealt within the articles or definitions section is that we saw the definition of "authorised person" which is in the Cybercrime Act. We are satisfied that the way it has been amended or included in the Cybercrime Act

has included the Office of the Director of Public Prosecutions and we are quite happy with that. However, we submit that before it is acceded, that we accede what is already part of the Cybercrimes Act because it is already in place and it already covers these definitions, so long as we include the definition of “content data” and ‘cybercrime’.

If I may move on to Article 2. Article 2 is also included in the Cybercrime Act 2021 and is covered in section 5 of the Cybercrimes Act. We do not see the need to accede this because it is already covered. In fact, honourable Chair and the Members of the Committee, most of it is already covered.

Article 3 is already covered in section 6 of the Cybercrimes Act which deals with offences and penalties. Article 4 is already similar to the provisions of section(s) 6 to 8 of the Cybercrimes Act and the same for Article 5 which is covered in the provisions of computer systems and section(s) 5 to 8 of the Cybercrimes Act. We see a similar thing in Article 6 which is on misuse of devices. We see that it is already dealt with in section 8 of the Cybercrimes Act. The only suggestion that we submit to the honourable Chair and the Committee is that there needs to be a specific definition of “device”. For this Budapest Convention to actually work, we need the Cybercrimes Act to be amended so that there is a specific definition of ‘device’ in the Act, so that it is clear for usage by the people that most likely will be affected when this Act is commenced or is passed by government.

In respect of Article 7 which is related to computer-related forgery, we see that it has already been covered in section 9 of the Cybercrimes Act, but again we see that there is a need to establish intent for corporate bodies. Whilst the section is already present in the Cybercrimes Act, with the absence of intent for corporate bodies we do not do justice to Article 7 of the Budapest Convention because we need to make it clear. If the laws are not clear, it will be difficult for people to comply and if they do not understand, the laws will not work.

Article 8 deals with computer-related fraud. We submit that, we make the same reservations that ‘intent’ needs to be clearly defined. If intent for corporate bodies is defined in the Cybercrime Act, it would do justice to Article 8 of the Budapest Convention.

In Article 9 which is offences related to child pornography, if you look at the amendment of ... commencement of the Cybercrimes Act 2021, the subsequent amendment is that in section 37 it made consequential amendments to the Juveniles Act. Now, previously the Office of the Director of Public Prosecutions had been prosecuting offences relating to child pornography using the Juveniles Act. While that is a consequential amendment in the Cybercrime Act 2021, in order to properly accede Article 9, our submission is that this Article needs to be amended in the Crimes Act 2009.

The reason why we submit that is because the Office of the Director of Public Prosecution has been in place for some time - it has been in place for many years. It would be the best office to deal with these particular charges. The Office has already prosecuted using this particular charge under the

Juveniles Act in *State vs Koronibau*, which is in the table. We respectfully submit that we do not need to accede this section because we can amend the existing laws - we can amend the Crimes Act 2009.

As for Article 10 we respectfully submit Mr. Chairman and honourable Members of the Committee that there is no need to accede to this Article because we already have relevant provisions in place in the Copyright Act and the other Conventions that Fiji is a party too. Those existing laws can be used to deal with Copyright Infringements.

As for Article 11 which is on Aiding and Abetting, we respectfully submit that there is no need to accede and this is provided for in the actual Article that it is not compulsory to accede to this section. However, if the Committee is minded to accede then we respectfully submit that we should use either the Cybercrimes Act 2021 that is already in place or we could use the Crimes Act 2009 that is already in place.

As for Article 12, which is corporate liability, we do not want to go extensively on this issue because if we deal with what I had submitted earlier on intent of corporate liability, we would cover corporate liability in Article 12. Sections 9 to 10 of the Cybercrimes Act already deals with offences that include corporate bodies but if we are not clear on what 'intent' is, it makes it difficult for corporate bodies that later will be charged under this offence. We need to have a balance between those who have been charged and the rights of the citizens that stand to be affected by this section, and the balancing act needs to take into account the provisions of the Companies Act 2015 and its regulations.

Mr. Chairman, Sir, and honourable Members of the Committee, these are my submissions and I will now move on to the others members of my Committee.

MS. L. MAUSIO.- Thank you Ms. Rakai. Mr. Chairman, Sir, and esteemed Members of the Parliamentary Standing Committee, my name is Ms. Lilian Mausio and I will be making submissions on Article 13 through to Article 24.

Regarding Article 13, as my colleague has said, we respectfully submit that we will not need to accede to this particular Article because it is already provided for in sections 5 to 12 of the Cybercrimes Act 2021 and these have already created sanctions and measures through the offence creating provisions.

With regards to Article 14, we respectfully submit that we do not need to accede because this has already been provided for in section 15 of the Cybercrimes Act 2021.

Article 15 requires parties to uphold the protection of human rights and liberties. These include rights arising out of obligations undertaken under various human rights treaties, and these treaties are mentioned in Article 15 of the Convention including the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms and also the International Covenant on Civil and Political Rights (ICCPR).

These two Treaties and Conventions although universal Mr. Chairman, Sir, do not reflect this new technological era that we live in, nor the novel problems arising out of it, one of the main ones are surrounded by issues of privacy of individuals. For instance the European Convention only makes reference in passing to the right of respect for one's private and family life, home and correspondence and that no public authority shall interfere with this right. On the other hand the ICCPR provides for protection against arbitrary or unlawful interference with one's privacy. Since these Treaties came into force, new technologies have emerged therefore falling outside the scope of the aforementioned Treaties and their privacy protections. Key notions such as the definition of privacy, the definition of correspondence and what constitutes interference in the modern context, are therefore ambiguous in the light of these technological advancements.

Local legislations such as the Cybercrimes Act 2021 will need to properly define the meanings and the ambits of these terms. Furthermore, Article No. 15, does not clarify what procedures exactly are needed to safeguard human rights, and parties are left to balance such procedures against potential human rights issues specifically privacy, Mr. Chair. This is worrying as it creates a lacuna for instance in a country which may have a poor record of safeguarding privacy protection.

In upholding the spirit of this Convention, any local legislation whether already in force or yet to be enacted must take up the mantle of explaining the scope of, and providing for procedural safeguards that protect the public from potentially, intrusive enforcement mechanisms. It can do this by clarifying what constitutes accessing enforcement surveillance and defining important terms such as privacy and the aforementioned terms. That being said, Mr. Chair, we are aided by case laws from other jurisdictions which seek to address the concerns above. An example of this is when the European Court of Human Rights, in the case of Copland and United Kingdom, held that the telephone data, emails, internet use and data stored on computer servers all fall within the privacy production rights under the treaties mentioned in Article No. 15.

With regards to Articles No. 16 and 17, it is our submission that they are already provided for in sections 18 and 19 of the Cybercrimes Act however these provisions need to have strict guidelines for the instances that they are issued without the sanction of the court. The Committee needs to balance the need to apply this provision with that of the individual rights and the need for a balanced investigation.

Articles 16 and 17, requires parties to adopt legislation instructing people and businesses to preserve data when ordered to do so by authorised persons. Article 16(2) requires a person to preserve such data transmission for an adequate period of time while Article No. 17 goes further by requiring data to be preserved regardless of the involvement of multiple service providers. Again, Mr. Chair, this creates a tenuous line between effective enforcement procedures and privacy of individuals. Without proper procedural safeguards in place the scope for this article could be used by authorities potentially to enforce surveillance or policies unrelated to actual cyber related crimes. Any local legislation must therefore provide for definitions and scopes to avoid the concerns that we just raised with regards to these articles.

Moving on to Article 18, it is already set out in section 21 of the Cybercrimes Act although this provision should be amended and be confined to a Court Order, and not extended at the discretion of the Police or authorised officers. This sort of provision can lead to abuse of power potentially and can cause irreparable harm to the reputation of individuals and businesses that are being prosecuted.

With regards to Article No. 19, it is our respectful submission that this provision is already set out in section 21 of the Cybercrimes Act. We would propose that this section of the Cybercrimes Act be deleted and instead, that it be confined to a Court Order. Article No. 19, allows the search and seizure of stored computer data. It specifies how authorised persons may monitor data transmissions but opens up the possibility of unnecessary intrusion into individual lives and matters unrelated to any potential crime because the scope of the article is wide and encompassing. The Convention needs to add an addendum and subsequently any local legislation enacted or to be enacted, would also need to add an addendum or ideally make a footnote, setting a definitive standard or guidelines so as to prevent any unnecessary intrusion or surveillance.

With regards to Article 20, we respectfully submit that this is already provided for in section 22 of the Cybercrimes Act. Article 21 is also already set out in Section 23 of the Cybercrimes Act. Article 20 in particular allows authorised persons to conduct real time collection of traffic data while Article 21 provides for interception of content data. The Convention does not define what 'content data' means but it is implied that it is a subset of traffic data.

Our local legislation needs to provide a definition of content data as supposed to traffic data. This is because it will enable authorised persons or law enforcement to either enact or adhere to specific guidelines when intercepting or collecting data transmissions. Again Mr. Chairman, this ties in with the privacy protection issues that we have raised earlier. The power given to law enforcement regarding surveillance in these two articles is substantial, therefore they should be complemented with specific guidelines that would curtail any possibility of unnecessary intrusion into the lives of private citizens or privacy rights violations.

It is our respectful submission with regards to Article 22 that this is already set out in section 3(1) of the Cybercrimes Act. Article 23, on the other hand is also already set out or realised in section 24 of the Cybercrimes Act.

Finally Mr. Chairman, my last submission with regards to Article 24 is much the same as my submission with regards to the other articles, in that many of these Articles have already been realised by way of the sections in the Cybercrimes Act. This is similarly so with Article 24 because section 25 of the Cybercrimes Act mirrors the spirit of these Articles.

Those are my submissions Mr. Chairman. I will now hand over the podium to my colleague, Ms. Bogitini. Thank you very much for your time.

MS. L. BOGITINI.- Mr. Chairman and honourable Members, my name is Lavenia Bogitini and I will now speak on Articles 25 to 37. With respect of Article 25, it is our respectful submission that these provisions has already been set out in section 30 of the Cybercrimes Act 2021.

With regards to Article 26, we also submit that this Article has already been provided for in Section 26 of the Cybercrimes Act. In terms of Article 27, it is our respectful submission that in terms of procedures pertaining to mutual assistance requests, the Budapest Convention allows for a party to refuse extradition under certain circumstances such as crimes constituting political offences or those that may prejudice a nations interest.

The provision however, does not clarify what type of offences qualify as political in nature or which they will consider prejudicial. This provision may become ineffective simply due to the different interpretations of what constitutes a political offence. The Convention needs to provide more detailed guidance as to what types of political offences or prejudices will legitimately justify a refusal to cooperate and who will render that decision. The Conventions should either provide additional guidance to signatories or set the standards itself, to ensure timely and efficient investigations through international cooperation.

Mr. Chairman, with regards to Article 28, this has already been set out in section 27 of the Cybercrimes Act. For Article 29, this has already been set out in section 28 of the Cybercrimes Act 2021, however this particular article creates a dilemma regarding dual criminality. As this particular Article does not require dual criminality as a condition for mutual assistance for the preservation of data. This creates challenges in the context of cybercrime where one jurisdiction may not recognise the relevant conduct as an offence at all. This raises a few concerns in terms of the preservation of data. Firstly, would this imply that one country has the right to interfere with the privacy of the citizens of another country. Furthermore, does this suggest that one country may impose onerous requirements to investigate crimes of the citizens of another country. Mr. Chairman, with this particular Article, we must strike a balance between the Mutual Assistance Act of Fiji, the Cybercrimes Act as well as the Crimes Act, when dealing with mutual assistance.

In terms of Article 30, Mr. Chairman, this Article has been set out in section 29 of the Cybercrimes Act, whilst Article 31 has been set out in section 30 of the Cybercrimes Act 2021. Article 31 relates to mutual assistance regarding the accessing of stored computer data. There is no provision in respect of specific grounds of refusal. This Article is one of the most intrusive requests of the Convention, however within the Convention it appears to be deferred to existing arrangements or domestic laws. The Convention does not provide any model procedures or standards in which this can be adapted by the signatory country whilst also being consistent with the Convention for the Protection of Human Rights and Fundamental Freedoms.

Mr. Chairman, however, I must submit that the grounds for refusal are covered in Articles 25 and 27, however, it is more specific to mutual assistance regarding the accessing of stored computer data as laid out in Article 31. In terms of Article 37, this has been set out in section 31 of the Cybercrimes Act.

Sir, for Article 33, this has been set out in section 32 of the Cybercrime Act. Mr. Chairman, Article 33 relates to mutual assistance in the real time collection of traffic data and this is specifically stated to be governed by the conditions and procedures provided under domestic laws. The preservation of data and traffic logs are only useful in the investigation of a hacker where real time evidence can be collected and communication potentially intercepted. However, real time evidence collection and interception of communications may requires certain procedures for a warrant under section 22 of the Cybercrime Act 2021 and this may render Article 33 ineffective in practice. Therefore, there needs to be a balance between safeguarding of the rights of individuals and allowing for an expedited application.

In terms of Article 34, this have been set out in section 33 of the Cybercrimes Act. In Article 35 this has also been set out in Section 34 of the Cybercrime Act 2021. For Article 36, this particular chapter in the Budapest Convention deals with the final provisions of the Convention, however, there is an obvious failure to include any follow-up measures to ensure that ratification is followed by compliance.

Mr. Chairman, those are my submissions with regards to Articles 25 to 37. Thank you.

MS. M. RAKAI.- Mr. Chairman and honourable Members of the Committee, if you look at our submissions on Article 38 to Article 48, we submitted that we should accede the provisions but subject to the concerns that we have raised in our table. Those are the pertinent issues that we wish to bring to you Mr. Chairman and the honourable Members of the Committee this afternoon.

MR. CHAIRMAN.- Thank you for your very informative dissection of the Articles of the Convention and its relevance to the Cybercrimes Act 2021 and the Crimes Act 2009. I now give the floor to the honourable Members who wish to raise any questions.

HON. L.S. QEREQRETABUA.- Mr. Chairman, I just want to say thank you very much for all the work. I can see that you really went through this with a fine toothed comb and magnifying glass. It has been a real eye opener and a little bit scary if I can say. It sounds like a Police State in the making, so thank you very much and we definitely will be in touch.

HON. P.W. VOSANIBULA.- Mr. Chairman, I would also like to thank the team for the legal dissection they have provided us this morning. Throughout the week, we have not seen the Cybercrime Act that clearly. We are thinking of going back to it after this, but now you have come in with those as we think globally and act locally.

HON. S. ADIMAITOGA.- Mr. Chairman, I just want to thank you for such an empowering and educational submission this morning. It has empowered us and it is an opening for us on what to do next.

MR. CHAIRMAN.- I do not have any questions. It is a very enlightening and comprehensive review as I have alluded to. I wish to thank you again and if we do have any further questions or queries, you will avail yourselves for that. With those few words any departing comments.

MS. M. RAKAI.- Mr. Chairman, it is an honour to be invited to submit and we welcome any question. From the words of the President, Mr. Clarke and the Council, if there is any further assistance we are available to come and assist the Committee. We thank you for inviting us. We come to Government Buildings to go to Court, so it is quite new for us to come to Government Buildings to submit to the Committee and it is a great honour to be before you this afternoon.

MR. CHAIRMAN.- Wish you all a blessed afternoon and the week ahead of you.

The Committee adjourned at 12.08 p.m.

# **[VERBATIM REPORT]**

## **STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE**

### **Convention on Cybercrime**

**INTERVIEWEES/SUBMITTEES: FICAC; UNOHCHR; FIU;  
CCF**

**VENUE: Big Committee Room and Small  
Committee Room, Parliament**

**DATE: Monday, 3<sup>rd</sup> October, 2022**

**VERBATIM NOTES OF THE MEETING OF THE STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE HELD IN THE COMMITTEE ROOM (EAST WING), PARLIAMENT PRECINCTS, GOVERNMENT BUILDINGS ON MONDAY, 3<sup>RD</sup> OCTOBER, 2022 AT 9.31 A.M.**

**Interviewee/Submittee:** Fiji Independent Commission Against Corruption (FICAC)

**In Attendance:**

- |                          |   |                                       |
|--------------------------|---|---------------------------------------|
| 1) Mr. Rashmi Aslam      | - | Commissioner                          |
| 2) Ms. Stephanie Smith   | - | Training and Public Relations Officer |
| 3) Mr. Frank Tora        | - | Chief Investigator                    |
| 4) Mr. Aporosa Vuinakelo | - | Digital Forensic Investigator         |
- 

MR. CHAIRMAN.- A very good morning to you all and it's a pleasure to welcome everyone, especially the viewers watching this proceeding. For your information, pursuant to Standing Order 111 of the Standing Orders of Parliament, all Committee Meetings are to be open to the public, therefore, please note that this submission is open to the public and media and is also being streamed live on Parliament's website and social media online platforms and the Parliament Channel on the Walesi Platform. For any sensitive information concerning the matter before us this morning that cannot be disclosed in public, this can be provided to the Committee either in private or in writing.

Please be advised that pursuant to Standing Order 111(2), there are only a few specific circumstances that allow for non-disclosure and these include:

1. National Security matters;
2. Third party confidential information;
3. Personnel or human resources matters and
4. Committee Deliberation and development of committee's recommendation and reports.

I wish to remind honourable Members and our guests that all questions to be asked are to be addressed through the Chair. This is a parliamentary meeting and all information gathered is covered under the Parliamentary Powers and Privileges Act. Please bear in mind that we do not condone slander or libel of any sort and any information brought before this Committee should be based on facts. In terms of the protocol of this Committee meeting, please minimise the usage of mobile phones and all mobile phones to be on silent mode while the meeting is in progress. Allow me now introduce the Members of my Committee.

(Introduction of the honourable Members of the Committee)

Today, the Committee will be hearing a submission on the Convention on Cybercrime otherwise known as the Budapest Convention. For the purpose of the viewers that are joining us this morning, please allow me to give a brief explanation on the Treaty. The Convention on Cybercrime, also known as the Budapest Convention provides a comprehensive and coherent framework on cybercrime offences and electronic evidences. It serves as a guideline for any State developing comprehensive national legislation against cybercrime and as a framework for international cooperation amongst States Parties.

To date, the Convention has 67 member States which includes Australia and Tonga from the South Pacific region. Pursuant to Article 37 of the Convention, any other State, such as Fiji, can become a Party by accession if the State is prepared to implement the provisions of the Convention and upon invitation to accede to the Convention after consultation and approval of Parties.

With the extreme effects of global cyber threats and attacks on critical sectors such as finance, ICT, energy, water, emergency services, public safety, health, public services, aviation and e-government infrastructure, becoming a Party to the Convention will enhance Fiji's ability to combat cybercrime, with the international support and assistance particularly in relation to continued capacity building, to better equip

Fiji's criminal justice authorities, including the judiciary, prosecution and law enforcement agencies.

Ladies and gentlemen, before us this morning we have Fiji Independent Commission Against Corruption (FICAC) and I now request the Commissioner, Mr. Aslam to introduce his team and to begin his submission after which, there will be a question and answer programme.

MR. R. ASLAM.- Mr. Chairman, with me, two investigators are here, Mr. Frank Tora, the Chief Investigator and Mr. Aporosa - both are experts in extracting electronic evidence and they are in charge of the Digital Forensic Unit of the Commission. Ms. Stephanie Smith is our Media Officer. Before I commence, may I hand over the written submission, which I will be reading shortly. First and foremost, we thank the Committee for inviting the Commission to make its submission.

This is important at this juncture as the Committee endeavours to provide the necessary recommendations to the Parliament of Fiji on the importance of joining the Budapest Convention as a State Party. Over the years information technology had changed the human lives drastically and will surely continue to impact all of us in the future as well. It has more often made lives easier in many aspects. It revolutionised the human interaction and methods of communication. Human interactions have become more complex, sophisticated and also overcome the distance and time variance that were in place a few decades ago. With such technological advancement in the cyberspace, the conventional criminals and the fraudsters too have evolved and become cyber complicit. Cyber universe has become an opportune conduit to advance the fraudulent and criminal activities on a different and larger scale. Many individuals and governments fell victim to cybercrimes losing millions of dollars. There was and is, a dire need to tackle the ever increasing criminal activities via internet and computer networks.

Cybercrimes have no border. No distance or geographical barriers could prevent or slow down cybercrimes. It can affect anyone regardless of his or her race and religion. It can affect multiple countries within a split-second. As such combatting cybercrimes need a collective global effort, comprehensive and co-operative strategies. Budapest Cybercrime Convention is a joint effort designed to address those prevalent issues by the Council of Europe and other States Parties. Cybercrime Convention is the bastion and provides the strategic framework to combat cybercrimes effectively.

Building up to this stage and other Cybercrimes Act, No. 3 of 2021 – prior to the enactment of the Fijian Cybercrimes Act, the only provisions available to tackle cyber offences were under section(s) 336 to 346 of the Crimes Act 2009. Some procedural support were also provided under the Criminal Procedure Act 2009 and the Prevention of Bribery Act, however, they were of limited use due to lack of capacity to provide necessary support from the service providers and users. Nevertheless it is noteworthy that the Commission within a limited legal framework, had successfully investigated and prosecuted several largescale corruption offences committed in tandem with cybercrimes.

Two cases are worthy to note at this juncture. The first case is FICAC vs. Ana Laqere and Others - the case involved several officers of former PWD and some private companies. The officers were working in the accounts section of its central and eastern division offices, situated in Walu Bay and colluded with private companies, owners and directors to raise bogus procurement orders and managed to syphon out millions of dollars from PWD. They manipulated the Financial Management Information System known as FMIS to an unprecedented level in diverting public funds to those companies. In addition we also noted that the perpetrators were stealing the identity of some reputed companies and used those company quotation forms through forgery and committed some form of identity theft.

Many reputed companies fell victim to the scam, however, there was no specific offence existing at that point in time to tackle these complex scenarios. They all were charged under Crimes Act for abuse of office and obtaining financial advantage. All the accused persons from PWD were convicted before the High Court and currently serving imprisonment sentences. Some cases are still pending before the court against private companies. When the investigations commenced, we realised that most of the physical documentary evidence relating to fake procurements were destroyed, however, we managed to reconstruct them using the FMIS data and information.

This is one of the first examples that the Commission realised the extent of cybercrime activities of corruption committed by public servants and the need to have a strong legal framework to battle corruption related cybercrimes. The second example is FICAC versus Viliame Katia, the case where the former Deputy Official Receiver squandered more than \$4 million from the Official Receiver's Account. One of his modus operandi was to use the computer system available in the Official Receiver's Office to create fake debtors and creditors accounts and managed to convince his supervisors and the banks to make payments which he directly benefited from. As such cyber related corruption involving large sums of public money was becoming prevalent and there was a need to have a strong legal framework that was compatible with the international standards as stipulated in the Convention.

Fiji commends the preparatory work to enact a cybercrime legislation, a few years ago with the stakeholders collaboration and also with the help of experts, consultants and representatives of the Council of Europe. I am very proud to say that the Commission engaged in this process and contributed well at every important stage in that process. At this stage I must take this opportunity as well to acknowledge the contribution rendered by the then consultant of the Fijian Government, Mr. Jayantha Fernando and his colleagues from the Bureau of Cybercrime Convention of the Council of Europe, without whose guidance the journey would have been impossible.

Fast forward to the present day, we now have a Cybercrime Act ready. We also took part in the recent assessment by the Council of Europe and now we are eagerly waiting to make use of the provisions of the act to strengthen our fight against corruption. As I said before, cybercrime or use of internet and digital devices are a very common way of committing corruption offences and almost all investigations now have a cybercrime component. In this regard the Commission has established a specialised unit called Digital Forensic Unit, with expert investigators in extracting digital or electronic evidence.

In terms of the salient features of the Cybercrime Act, the Act comprehensively addresses the salient features of the Convention. The issues have been addressed under three key areas:-

1. The substantive criminal law including the legal definition of certain important technological terms;
2. The procedural law with reference to cybercrime investigation and collation of electronic evidence in relation to any crime;
3. The international cooperation.

It is not my endeavor to speak in detail about the features of the Cybercrimes Act however, as noted by our consultant and experts we can proudly say that the Act is one of the robust statutes available hitherto, in the Pacific Region to combat cybercrimes.

The Convention was considered as a reference model and incorporated various cybercriminal and conducts under the domestic law as criminal offences. It provides procedural powers to investigate and prosecute cybercrimes and also safeguards the rights of the public at large. The effective international cooperation among the stakeholders of criminal justice is imperative, as the criminal cybercrimes are often multi-jurisdictional.

Human Rights and democracy strategy - in addition to the general measures safeguarding human rights, it effectively addresses women and children's rights as well. Women and children are often exploited viciously by cybercriminals. The Cybercrimes Act provides sufficient tools to combat them effectively. Severe penalties imposed for child pornography are an example.

Finally, the accession - we strongly support Fiji's accession to the Convention. It will connect Fiji with the global efforts of fighting corruption and cybercrime, and will also provide several other benefits. Fiji is a commercial hub in the South Pacific and it is important to provide a safe commercial platform for all parties involved in commercial activities by providing a safe cyberspace. Women and children must feel safe in the cyber environment. Fiji can also benefit from international corporation immensely through capacity building. Those are our submissions, Mr. Chair.

MR. CHAIRMAN.- Thank you, Mr. Aslam for the very insightful report on the Cybercrime Act and also the evidence where you have given us some public examples. I now ask the honourable Members, if they have any questions for the team from FICAC?

HON. L.S. QEREQERETABUA.- If I may, Mr. Chair, my question I guess or my comments is in regards to human rights. As you know our own Constitution basically says that we have the right to freedom of expression and right to privacy or fundamental human rights recognised under the 2013 Constitution of the Republic of Fiji. My fear is that (and I would like to know what you think), acceding to the Convention could give unusual rights to certain institutions in Fiji to search and seize, and you also have the right to privacy of our homes and so forth. So if your investigators are now given the power to go and search and seize, basically walk into someone's home (of course with a warrant) but what are your thoughts on human rights and the rights to privacy under our Constitution?

MR. R. ASLAM.- It is a very important question that the honourable Member was asking. Of course the Convention has given tools to the investigators to be used. Does it infringe their right to privacy or their right to expression under the Constitution? The short answer is, no. The long answer is, it is not a new phenomenon in Fiji - these tools are already available. What it provides is further benefits or further tools in which we can streamline the powers of the investigator. In fact it does not make the investigators or any institution more powerful - it makes the institution more responsible.

For example, the other matter is that all the powers to be executed under the Cybercrimes Act are supervised by the Judiciary. It cannot be conducted by the organisation on its own so there is always the mechanism of supervision, there is another mechanism of challenging that particular activity of the organisation by bringing the matter before the Court of Law immediately, and there are other provisions under the Criminal Procedure Act safeguarding the rights of the accused persons. I can provide further examples, particularly where the rights of the suspects have been safeguarded, that is one aspect. The other aspect Mr. Chair, is that when it comes to human rights, of course there are certain limitations if they are not unfettered discretions of a person. At that point in time, the Judiciary or even for us as a law enforcement agency, we will have to undertake a balancing act and see whose interest are we going to privatise.

For example, let us say, it is a child phonographic matter. Obviously we know that there are damning evidence in one persons' computer or a mobile phone, and the person is not ready to cooperate, citing his right to privacy - who are we going to protect here? As a nation, as a Parliament, as a law enforcement agency and as the Judiciary, at that point in time, I think we will be able to create certain precedents as well as jurisprudence in a Court of Law. Anyone, including the suspect, can challenge the extraction of evidence by quoting their Constitutional rights but the Judiciary will exercise its general discretion at the end of day, in which way the extraction of that particular evidence must be used whether it really infringes a person's human rights. Even if it infringes, whose interests at the end of the day should be important, so it is a balancing exercise. Regulations are there on the Cybercrimes Act and we are quite confident that it will not be misused by any parties.

HON. DR. S.R. GOVIND.-Thank you, Mr. Aslam for the comprehensive presentation. As you have said, cybercrime in itself is such a complex issue with the increase in technological advancement, I think it will become more complex. Currently, you have said you have some capacity within the agency but once this is ratified and with the implementation of the Convention, how do you see the capacity within your department plus others? I am not sure whether you are using some private sector as well in your investigation but how do you see this capacity to be advanced on that because it is a big issue.

MR. R. ASLAM.- Mr. Chairman, thank you for that question. It is a very important and prevalent question right now. In terms of internal capacity, we are forever involved in the training of our officers, we keep on equipping our office and bringing necessary policy matters to safeguard the digital evidence that we are extracting. That does not mean that we are perfect, of course we have realised that there is a lot of room to improve within our organisation in terms of extracting digital evidence. If the Cybercrimes Act comes in and then we see that there has to be more advancement and more building on our capacity further, we will need more manpower, more expertise, and more equipment because obviously, there has to be a 24/7 contact point that is connected to the international platforms. To provide that kind of support services globally, we really need to have highly qualified expert officers and the equipment with us. We need to build up ourselves to that point and we are not perfect.

The other point is the private sector. Without the service providers I do not think we can implement any of these measures particularly the private companies and the public entities that provide services. We do have some working relationship with them but I must say at this point in time that we are not fully satisfied with the level of cooperation, with the level of expertise they have, the equipment and the time framework that they provide the support.

Mr. Chairman, if I may respectfully suggest at this point in time, it is very important to make sure and also listen to the private companies who are providing services, whether they are really ready. It is not about the readiness *per se* it is about the willingness, because the equipment and the expertise we need does not take long to build up. It

just needs to have the willingness to cooperate with the law enforcement agencies that is where we see the problem. I hope I have answered your question.

HON. DR. S.R. GOVIND.- Mr. Chairman, just a supplementary question. Is there a global agency which has expertise and capacity building like in the UN system or non-UN, is there an agency which you work with globally?

MR. R. ASLAM.- Mr. Chairman, the second additional protocol in Cybercrime Convention specifically addresses on capacity building. If we accede the Convention there are experts in the Council of Europe who will provide us the capacity building. Yes, the Council of Europe. I also understand that the UN is also working on it and at the moment in Singapore there is a centralising agency and they persist all other agencies in cybercrime matters. We also have some contact with them and I am confident that they will provide the necessary capacity building to us.

MR. CHAIRMAN.- Thank you, Mr. Aslam. We have heard from other submitters that it tends to be a 24/7 operation to tackle cybercrime as a whole. I do not have any question - honourable Adimaitoga?

HON. S. ADIMAITOGA.- Through you, Mr. Chairman, you have stated that women and children are often exploited viciously by cyber-criminals and the Cybercrimes Act provides sufficient tools. Can you explain further on the sufficient tools that you have mentioned to deal with this effectively?

MR. R. ASLAM.- There are two types of laws in the Cybercrimes Act - the substantial law which is covered under sections 5 to 14 and the procedural law from section 15 onwards. If I may just take an example, section 10 speaks about computer related extortion and fraud. It is a very wide section. We have seen some incidents in the past which I think the Fijian Police investigates under their Cybercrimes Unit where women were held at ransom and threatened that certain photographs taken in private would be exposed. That is one of the examples which is clearly covered under section 10 of the Cybercrimes Act as well.

If the substantial law is not sufficient under the Cybercrimes Act we can always fall back to the Crimes Act and for example, annoying a person or becoming a menace through cyber means, by messaging, et cetera. If the Cybercrimes Act does not provide an offence what it provides is a clear procedure as to how we can extract those evidence and then charge the person under the Crimes Act. It is quite comprehensive in that way and it provides enough room to the law enforcement agencies to tackle this type of issues. The other example, of course, is child pornography as I had mentioned before.

MR. CHAIRMAN.- Thank you, Mr. Aslam. Honourable Members, as there are no further questions, I wish to sincerely thank you and the team for availing yourselves and if we should have any other pressing questions in the not too distant future, we seek your indulgence to provide us that information. With those few words, I wish you all a blessed day and thank you once again.

The Committee adjourned at 11.43 a.m.

The meeting resumed at 11.28 a.m. [in the Small Committee Room (SCR)]

**Interviewee/Submittee:** United Nations Office on Drugs and Crime and the United Nations Office of the High Commissioner on Human Rights (UNOHCHR)

**In Attendance:**

Miss Releshni Kumar : Representative UNODC & UNOHCHR

MR CHAIRMAN.- Ladies and gentlemen, before us this morning we have the representative from the United Nations Office on Drugs and Crime, and the Office of the United Nations High Commissioner on Human Rights, Miss Releshni Kumar. You can present your submission, after which we will have a question and answer session.

MS. R. KARAN.- Mr. Chairman and honourable Members of the Committee, my name is Releshni Karan, just to correct for the record. Thank you for inviting us to present our joint submission to the Standing Committee. We are presenting this joint submission on Fiji's intention to accede to the Council of Europe Convention on Cybercrime, also known as the Budapest Convention.

The United Nations Human Rights Office and the United Nations Office on Drugs and Crime welcomes the opportunity to comment and provide guidance on the Budapest Convention through oral submissions. We appreciate the stance that Fiji has taken in inviting the views of stakeholders through a meaningful consultative process as has been presented. In recent years, there has been a search of cybercrime laws around the world, some of which has been overly broad and these broad laws tend to undermine human rights as well. It is understood that there is a risk that computer networks and electronic information may also be used for committing criminal offences, and that evidence relating to such offences may be stored and transferred by these networks.

We recognise and encourage cooperation between States and private industry in combating cybercrime and the need to protect legitimate interest in the use and development of information technologies. However, we believe that an effective fight against cybercrime requires increased, rapid and well-functioning international cooperation in criminal matters, which is in light with the international Human Rights law. An international Human Rights law dictates that the interest of law enforcement are subject to respect for fundamental human rights. These are enshrined in the 1950 Council of Europe Convention for the protection of human rights and fundamental freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international Human Rights Treaties.

Fiji has ratified all the core nine international Human Rights Treaties and is therefore bound to follow the provisions. Fiji, with a population of over 900,000 has more than half of its population using the internet of some sort, with the majority being of course Facebook users. Making the internet safer and protecting internet users has become integral to the development of new services as well as government policy. At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of the Government authorities, the private sector as well as the citizens.

The Fiji Government has a duty to protect people from criminal activities carried out through computers and the internet, but that should not come at the expense of people's fundamental rights. Our submissions, therefore, focus on general comments around the need to strengthen domestic legislation in order to assist in your decision on whether or not to accede to this Convention. The national legislation should have strong safeguards for the protection of human rights. At the outset, this is currently not a UN legal instrument. It is not a United Nation's

instrument on cybercrime. Therefore, both ONCHR and the UNODC can only provide guidance that can inform this Committee on areas to strengthen in domestic legislation before you decide to accede to the Convention.

We are not advising in any way whether Fiji should or should not accede to this Convention. We are providing this guidance to assist you to make an informed decision. The Budapest Convention was adopted on 23<sup>rd</sup> November, 2001, and entered into force on 1<sup>st</sup> July, 2004. The principle objectives of this Convention are to harmonise national legal frameworks, support cybercrime investigations and enhance international cooperation to combat cybercrime. I will not bore you with the rest of the provisions because by now I believe you all know it by heart probably.

Fiji was one of the countries invited to accede to the Convention in December, 2021. The Cybercrime Convention poses three necessary obligations and these are:

1. To enact legislation criminalising certain conduct related to computer systems.

There is a list of crimes that each participating country must have on its books. The Treaty requires criminalisation of offences such as hacking, production, sale and distribution of hacking tools and expansion of criminal liability for intellectual property violations and all these crimes are found in Article(s) 2 to 11 of the Convention. Fiji will have to adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in Article(s) 2 to 11 are punishable by effective, proportionate and dissuasive sanctions which include deprivation of liberty.

2. To create investigative processes and procedures and ensure their availability to domestic law enforcement authorities including procedures to obtain electronic evidence in all its forms.

What are those processes? Where are those procedures? These need to be very transparent. It may require each participating nation to grant new powers of search and seizure to its law enforcement officers and by this I mean the Fiji Police Force or the law enforcement officers that would be requiring the search and seizure powers. They include the power to force an Internet Service Provider (ISP) to preserve a citizen's internet usage records or other data, and the power to monitor a citizen's online activities even in real time, so they could see what you are doing on your phone, they can see what you are doing in your computer, they can see the conversations you are having, so all these will have to have some sort of transparent processes and procedures in place first.

3. There is a need to create a regime of broad international cooperation including assistance in extradition of fugitives, sought for crimes identified under the Convention.

Basically it requires the law enforcement in every participating country to assist the police from other participating countries to the widest extent possible - there has to be some parameters on that as well. Does Fiji even have a say should a participating country ask for a Fijian citizen to be extradited and under this Convention, those parameters need to be defined in domestic legislation. Your domestic laws need to state what grounds they would be and if it is open-ended then there is a real danger.

Fiji has met some of its requirements through the enactment of the Cybercrime Act 2021 which has criminalised conduct related to computer systems and providing penalties including in Part 5 – the power to seize and search and the power to monitor a person’s online activities in real time, under a court order. Now Part 6 of the Crimes Act 2021 also has provisions allowing for international cooperation. Some of the offences established in accordance with this Convention are deemed extraditable offences and they will be covered under Fiji’s Extradition Act 2003. It is reminded that double criminality is a requirement for extradition from Fiji and due to the specific nature of the offences under discussion, the relevance of section 3(2) of the Extradition Act 2003 may need to be reconfirmed.

Some general comments on this Convention. As procedural frameworks developed for cybercrime can be used to obtain evidence in investigations of any alleged crime possessing digital traces, strong human rights protections regarding access to and the use of these tools are key. Effective procedural frameworks in international law that enable access to this evidence in a timely manner are crucial for tackling the problem of cybercrime. However, access to their digital data can have a detrimental impact on human rights when covertly, which is possibly in a hidden form, or intrusively it is procured and potentially allows for the collection of a large amount of sensitive information that is collected, which is beyond the scope of investigation, as well as interfering with the privacy of third parties. As you know we do not only keep our information in the device, we also keep information of third parties, children, women, people we connect with, our colleagues. All of that information is in the data and the investigation must be clear in this respect of what is the scope of that investigation. It has to be proportionate and the investigative and procedural measures that affects human rights should be necessary and proportionate as well as legal.

Criminal investigations typically entail restrictions. Such restrictions, for instance to the right to privacy can only be imposed to pursue a legitimate claim. While the investigation of crimes constitute such a legitimate claim, it is essential that any investigative or procedural measures that constitute a limitation on human rights, it is necessary and proportionate in achieving that claim and it has to be the least intrusive approach that would be taken by the law enforcement officials.

Judicial authorisation and ongoing supervision over these covert investigatory measures is necessary. The absence of robust safeguards in the application of covert investigatory measures can undermine privacy, it can have a chilling effect on the freedom of expression, the freedom of association and other human rights. If there are no checks and balances, what citizens would be very fearful of is what to text the other person, or whether to text the other person or not. We will always have this fear that someone is watching so, this should not have that chilling effect on journalists for example, on government officials, on members of the Opposition for example, on media, on human rights defenders. It should not have that chilling effect and so to prevent that chilling effect, there has to be a very robust domestic legislation that protects these rights.

Interference of investigative and procedural measures with human rights, including the right to privacy, requires the existence of independent and impartial oversight and that is by the court of law. Any investigative measures that want information from electronic devices should be by a Court Order, it should

be by a Warrant and there has to be that judicial control over the application of such steps that the law enforcement agencies would take.

Now, the search and seizure method should be subject to robust safeguards and an independent oversight as well. The mutual legal assistance that is present as is required under the Convention, should be subject to dual criminality requirement as well. It should be subject to the approval of competent authorities in both States. Also, Fiji needs to decide that and should be able to decide what or who can be extradited? If there is a Fijian who has not broken any Fijian laws, should that person be extradited? Just because that person has broken the law in another participating country - those are some of the considerations that should be taken into account.

To guarantee the protection of human rights in cross border exchange of electronic evidence, a strong level of scrutiny is necessary for data requests. In mutual legal assistance procedures or in executing mutual legal assistance requests, States should apply the same level of safeguards as provided under the domestic laws, so the domestic laws need to be strengthened in this regard. The State should also be able to evaluate a request to ensure compliance with human rights and not just be obligated to provide this information from the participating country.

The obligation to provide mutual legal assistance should be subject to strict compliance with international human rights standards and it should include a responsibility for an executing State to evaluate the records using those standards. Fiji should be able to refuse the request on the grounds that it would put in its domestic legislation, for example, what if the State is seeking extradition of a Fijian person in Fiji, who is facing a death penalty? Fiji does not have the death penalty anymore but other countries do. What if the extradition is for that purpose? Should Fiji then allow it? It is these sorts of consideration. It is important to consider these issues because this will affect all Fijians.

Refusal of mutual legal assistance on such grounds can also include cases in which there is substantial reasons to believe that a person may be investigated or prosecuted on the grounds of political opinions, religious beliefs, nationality and in some cases, sexual orientation. As you know, being gay or being a lesbian is criminalised in a certain number of countries. What if his extradition and his request for data for that information is solely on that basis, so those parameters have to be established first - ethnic origin or other prohibiting grounds of discrimination - these need to be stated.

Privacy and civil liberty protections also need to be considered. When considering the adoption of the Budapest Convention, Fiji would need to take into consideration its international human rights obligations and adopt human rights considerations in its national legal framework. The right to privacy of correspondence is enshrined in the 2013 Constitution of Fiji and this principle applies to all forms of electronic data transfer whether by computer, telephone, fax, email or file transfer - these will all come into play.

In the past, Fiji has had instances of spying, or unauthorised surveillance by other countries which has caused a national debate on privacy laws. These privacy concerns have to be taken into account and it is paramount that any new legislative provision be consistent with international human rights standards, that protect the use of telecommunication services and the social media communications. The surveillance needs of the law enforcement authorities needs to be scrutinised as well.

The United Nations Human Rights Council has repeatedly affirmed that the same rights that people have offline should be protected online, in particular freedom of expression which is applicable regardless of frontiers and

through any media of anyone's choice. Freedom of expression is viewed as a right that includes and facilitates the enjoyment of other essential economic, social, cultural, civil and political rights, including the rights to freedom of peaceful assembly and association. All these freedoms can be practised online as well.

The content offences is something we have to be very careful of as well. As computers are becoming more and more intertwined with modern life, this will apply to a larger and larger proportion of crimes. If acceded to, the foreign police can require the Fiji Police Force to tap a persons' and listen in to their conversation as well. Should they be allowed to search his or her computer or should they be allowed to send this information to the participating country without knowledge of the person? These are the things that need to be looked at quite well before you decide to accede.

This Convention imposes this requirement that the domestic legislation should have the human rights safeguards. Any legislation should focus on offences that are specific to computer data and systems, and require explicit criminal law provisions due to the lack of protection provided by existing criminal laws. On that basis, only a narrow set of offences inherent to cyber space should be criminalised such as crimes against integrity, confidentiality and availability of data and systems, misuse of devices for the purpose of committing these crimes and where appropriate, a number of specific computer related offences such as computer fraud, computer forgery - these can be criminalised.

In addition, OHCHR suggests that any future agreement on cybercrime with any country should avoid including offences based on the content of online expression - these we call content offences. The cybercrime laws have been used in the past to impose overly broad restrictions on free expression, for example by criminalising various online content related to extremism, terrorism, hate speech, public morals and all of those. The provisions of any domestic legislation should try to avoid overly broad and vague terms because this can be interpreted to apply to improperly restrict conduct of States. The principles of legality and other legal certainty require criminal law provisions to be publicly accessible, clear, concise and precise in scope, so that individuals can reasonably ascertain which conduct is prohibited and which is not prohibited, and they can adjust their behaviour accordingly. Anyone using a phone should know if what they are doing is legal or not and they should not be confused in their minds whether it is legal or not legal for them to have that adjusted in their behaviour.

Now vague and imprecise definitions of offences leave room for arbitrary interpretation and they also risk infringement of human rights. To reduce these risks and to avoid over-criminalisation, any legal framework should try to define criminalised conduct in a very narrow and clear manner. Of course, there are terms used in place of the terms that are in the Conventions such as pornography and child pornography.

The term "child sexual abuse material" is increasingly used to replace the term 'child pornography' and the switch in terminology is based on the argument that sexualised material that depicts or otherwise represents children is indeed a representation and a form of child sexual abuse. It should not be child pornography because it risks insinuating that the act was carried out without the consent of the child or the guardian, and represents legitimate sexual material. Some of those terms will also have to be looked at.

Now, ambiguous terms such as 'political offences' is not defined in the current legislation and this represents a significant omission since an offence that is considered political in Fiji, might or might not be a criminal matter in another country or vice versa. The onus of deciding what is political in this space would then be undecided. Who determines what is political or not? Who determines that? It is paramount to ensure that any referral, extradition

or mutual legal assistance is done through a process involving judicial approval - it has to go through the court system and oversight.

Also it is crucial to have a reporting requirement and this is something that Fiji can consider where it requires instances of co-operation with other countries on foreign crimes. These crimes should be made public to ensure that law enforcement decisions can be subject also to civilians and journalists - check and oversight.

It is crucial also to look at dual criminality as a prerequisite for mutual legal assistance. It is crucial to consider the issue of mutual assistance in the real time collection of data and to integrate the definition of content data in domestic legislation; it is not there at this point in time. Legislation needs to integrate the need for dual criminality or for the underlining basis for suspicion to be a crime in the country in question. A dual criminality provision would require an activity to be a crime in both countries, not just one. It has to be a crime in both countries before one nation decides to enlist the police in another, to help investigations.

It can work both ways. If someone's information is asked for from another country and Fiji provides that, then that person should have been involved in a criminal matter here for the Fijian Police to actually extradite or give that information to the other side. Of course, Fiji can ask for extradition of a person sitting in some other country, provided that person has committed an offence in that country as well. There has to be dual criminality.

The legitimate work of civil society organisations, women organisations, human rights defenders, journalists, media and other actors pursuing the public interest, should be protected at all times. In a number of countries, cybercrime laws have been used to restrict lawful activities of a wide range of civil society actors, which are essential for transparency, accountability and the protection of human rights in democratic and pluralist societies. Overly broad and vague criminalisation of access to information, data and systems can limit and penalise legitimate access to information and disclosure, especially to whistle-blowers. Poorly constructed offences against confidentiality, integrity and availability of data can also risk impeding the work of cyber security researchers and academics. This can have a chilling effect on discovering information system vulnerabilities and putting users and businesses at higher risk of cybercrime.

Fiji should thus ensure that the provisions of its legislations will no doubt be reviewed and do not hamper legitimate activities notably of all the stakeholders - journalists, politicians, cyber security researchers and academics - and should not be used to prosecute whistle blowers. It is imperative that existing domestic laws that limit the work of human rights defenders, do not become even more restricted after Fiji accedes to this Convention, or cause a chilling effect on their legitimate work. Efforts need to be made to ensure that the domestic legislation is compliant with international human rights laws and standards, and allows all the stakeholders to operate without any undue restrictions.

The investigative measures and surveillance powers should be limited in scope as well duration. Fiji should take care to avoid risk of exposing individuals to arbitrary surveillance by law enforcement officials without adequate reason. Any future Convention that would come from the UN would require Parties to establish a clear scope and temporal limits for ongoing measures, concerning any form of access to production or acquisition of any types of private communications and personal data in criminal investigations - and you put in place measures to ensure that those limits are adequately respected and enforced.

There also has to be some sort of requirement on the internet service providers (ISPs) and their cooperation with the search and seizure of data. The ISPs cooperation with search and seizure of data without requiring police to reimburse them for the cost of that corporation should they be sued, is also infringing the rights of the ISP providers. We are a small nation with very few (ISP) providers, so we also have to look at the compensation, should something go wrong in these sort of instances. These are the things that may have these gaps in domestic legislation because in other countries, which are mostly the European countries that have ratified this, there are funds and resources to adequately compensate should there be some sort of overstepping the mark, if I may say. In Fiji, it may come through case law but it is advisable that it should be covered under domestic legislation.

That undermines one of the most important checks and balances in any democratic system when you do laws and it is the control over law enforcement, that the State maintains through its budgetary power of a person. Do you have the power to handle that, should something go wrong? This is cyberspace - we will look at cyber money as opposed to real money, we will look at crypto currencies, we will look at digital data that would be lost, data of an entire institution that can go missing - who pays for that?

There is also a need to protect privileged communications such as attorney/client communications or medical records if there is a doctor/patient privilege - those things should be protected. Protection of privileged communications between protected persons fosters important public interest, and the protection of the right to a fair trial. The lack of such protection can deprive suspects and other persons of effective legal representation of their interest. Fiji would also need to consider the provision of robust safeguards for the confidentiality of legitimate attorney/client and other privileged communications in accordance with international human rights law and standards.

Before I end my submission, Mr. Chairman, I would like to say that the United Nations is also working on a new Convention on Countering the Use of Information on Communication Technologies for Criminal Purposes. It will work with the European Council as well and their UN Member States. This new Convention is undergoing negotiation and it is being consulted at this point. The United Nations General Assembly has adopted a resolution, that the draft Convention is to be provided to the General Assembly at its 78<sup>th</sup> Session which will begin in September, 2023 and conclude in September, 2024.

Fiji may wish to have a look at that as well, if you do wish to accede to an international standard when it comes to cybercrime. There are of course, a number of Conventions of varying scopes that address the issue of ICTs in criminal purpose and cybercrime, but there is currently no United Nations legal instrument. There is an ad hoc committee that is going around doing these consultations. The text provides an overview of all the international instruments, recommendations and other documents that is aimed at countering the use of information and communications technologies for criminal purposes and it is found on the United Nations Office on Drugs and Crime (UNODC) website as well as the Office of the High Commissioner for Human Rights (UNOHCHR) website if you wish to have a look at the work of the ad hoc committee.

Mr. Chairman, that highlights the main issues that we wanted Fiji to consider before it decides to adopt the Budapest Convention. Thank you very much.

MR. CHAIRMAN.- Thank you, Ms. Karan, for that very informative and comprehensive report on the Convention and its relevance to human rights. Honourable Members, do you have any questions?

HON. L.S. QEREQERETABUA.- If I might, Mr. Chairman, just to thank Ms. Karan for that fantastic presentation. I know you have raised some red flags that I also heard from the Fiji Law Society presentation last week, and I absolutely thank you and your team for the advice. Are you able to share your presentation today, with the Committee?

HON. R. KARAN.- I can share the written submission to the Committee but it will take me some time because the UNODC focal point, Ms. Marie Cauchois, is not here in Fiji. She is in the Solomon Islands and I need her to say yes before I can send the official written response.

HON. L.S. QEREQERETABUA.- Thank you.

HON. DR. S.R. GOVIND.- Yes, I would also like to thank Ms. Karan, for a very comprehensive presentation focusing on human rights. This is just a general comment - there are some Conventions initiated by the UN, but some are also initiated by European Union and councils, so I would like to know what is the difference. What should a Member State do because Fiji is part of the UN and not part of the European Union but many Conventions are coming from the European Union, so what is the UN's views on this - it is a little bit confusing to us.

MS. R. KARAN.- We do not hold a view on how Fiji should look at the European Council or the EU Conventions that are coming out, but we would like you to have a look at how this Convention is made. The international conventions that come out of the United Nations are done through consultative approach. They take views of member States in the drafting process. They also take in the views of the civil society, business houses, and it also takes the views of the high government officials. The Budapest Convention may not have been that inclusive, therefore you will see that they have a very strong critical sort of component of law enforcement but there is no civil society at all involved in its making.

When you are trying to decide which Convention to go to, it is first imperative to look at what Conventions you have acceded to already, what you have ratified already. Fiji had ratified nine Core International Treaties which also involves the International Covenant for Civil and Political Rights (ICCPR). That has provisions that also apply to cyberspace, not quite explicitly but it does have those general provisions there and what extent of rights that need to be limited is also stated there.

We do appreciate Sir, that there is no UN Convention on Cyberspace yet but there is one that is being consulted and it may be prudent to perhaps wait this out and be involved in the process. Of course there are always criticisms at the processes and the way it has been done, but if Fiji wants to accede to an International Convention it needs to look at the principles and what is being said in the Convention. Right now you have the Cybercrime Act, you have the laws, you are trying to put your foot into that space and try to regulate that space in a very fair and legalistic manner. That is the start but there has to be those safeguards of human rights and these safeguards come from international standards.

To look at those international standards - the ones you have already ratified like the ICCPR and you look at the extradition provisions - all these provisions are in the ICCPR. You look at those and you adopt them. If there is something that is not consistent then perhaps it is prudent not to accede, but it is really the decision about the State whether they wish to accede to a UN Convention or whether they wish to accede to a Council of Europe Convention.

HON. DR. S. GOVIND.- Mr. Chairman, Sir, there is a draft legislation on Cybercrime. Were you consulted on that or did you give a report? Have you seen the draft legislation? Does it cover most of the issues that you have raised?

MS. R. KARAN.- Yes, we were invited by the same Committee for the Cybercrime Bill and we raised substantial issues with them. Unfortunately, not all has been accepted by the Committee but some provisions have been integrated and we thank the Committee for that. The Budapest Convention requires all domestic legislation to have the safeguards, so even if you accede to it, your acceding to the general provisions and then when it comes to the nitty-gritty part of it, the Convention says that extradition will be done from State A to State B, should there be requirement. Exchange of data can be exchanged between parties. There will be a requesting party then there will be a party which will have its law enforcement officials doing certain seizures and giving this information to the participating party. The nitty-gritty of that will have to come through the domestic legislation, through the regulations. So, if there is a need to say, search my phone, should I give this to the law enforcement agency? The legislations which is your Cybercrimes Act, your Police Act, your Online Safety Commission Act or the Extradition Act for example - all these legislations will look at different parts of this criminal offence and will tell me as an individual, as a Fijian citizen, whether I should just give my phone or should this come by court order, etc, so the submission basically is that Fiji needs to strengthen its domestic legislation from a human rights perspective in order to accede to a Convention like this.

This Convention is with the European countries. They have already set their domestic legislation and they have very stringent legislation where if something goes wrong there is a very high compensatory penalty. We need that as well.

MR. CHAIRMAN.- Any further questions, honourable Members. Time is against us. Thank you again, Ms. Karan for availing yourself. We hope that should we have any other pressing questions or need clarifications that you will avail yourself. We will look forward to Ms. Marie who has mentioned that she will forward us a written submission. With those few words thank you once again for your availing yourself, have a blessed day.

MS. R. KARAN.- We will provide the written submissions to the secretariat through the same channel.

The Committee adjourned at 12.11 p.m.

The Meeting resumed at 11.24 a.m. [in the Small Committee Room (SCR)]

**Interviewee/Submittee:** Fiji Intelligence Unit (FIU)

**In Attendance:**

1. Mr. Razim Buksh - Director of Financial Intelligence Unit
  2. Ms. Esther Sue - Manager Intelligence Unit
  3. Ms. Sharlene Wong - Financial Intelligence Analyst
  4. Mr. Lawrence Chandra - Senior IT Specialist
  5. Mr. Kritesh Bali - IT Systems Analyst Specialist
- 

MR. CHAIRMAN.- Ladies and gentlemen, before us this morning we have the Financial Intelligence Unit and I now request the Director Mr. Razim Buksh to introduce your Team Sir and you may start your submission immediately, after which we will have question and answer session. The floor is yours Sir.

MR. R. BUKSH.- Thank you, Mr. Chairman and honourable Members of this august Standing Committee, *bula vinaka* and good morning.

My name is, as Mr. Chairman mentioned, Razim Buksh. I am the Director of Fiji's Financial Intelligence Unit, the first Director established under the Financial Transactions Reporting Act. On my immediate right is Esther Sue, she is the Manager Intelligence, she looks at all the suspicious transactions and disseminations to law enforcement and she is also responsible for coordination and networking with not just domestic partners but with the international partner agencies; on her right is Sharlene Wong she is one of the Financial Intelligence Analysts at the FIU; on my left is Lawrence Chandra the Senior IT Specialist; and on his left is Kritesh Bali he is the IT Systems Analyst Specialist as well at the FIU.

I will try to make this submission as relevant as possible but at the same time making it interesting so that the Committee Members are able to understand the context of where we are making the submission. I have included several slides that are meant to be part of the submission before this Standing Committee and it is not necessary that I go over all the slides in detail. I will skip some of the slides and if the Committee wants us to revisit some of the slides I would be more than willing to do that but those can be considered as part of our submissions. The slides are very long but I will try to keep it to the 30 minutes assigned to us and we will keep some time for questions and answers.

The submission goes in three to four steps, I will give the context and I will talk about the substance of the submission. Our position is in relation to the Cybercrime Convention (Budapest Convention): what are some of the challenges and how these will fill in the gaps. I will also talk about some of the case studies, some more broadly and some very specific to cybercrime and cyber security related incidents. The Committees is appreciative of the work that we do in terms of the practical realities on the ground that the FIU is involved on a day to day basis.

Our role very briefly is to contribute to the prosecution investigation of financial crimes - whole spectrum of types of cases not just money laundering but it includes corruption, tax evasion, fraud, forgery, cyber-related cases as well.

The FIU is also centrally positioned to undertake credibility and background checks on behalf of Government entities and agencies. We implement preventative measures under the financial systems that as you and I approach a commercial bank or any financial system, it is the FIU that sets the customer on-boarding rules how the banks should on-board a customer and conduct financial transactions.

The FIU is also very well centrally placed and we look at Fiji's not just the FIU's but our national compliance with anti-money laundering standards. We are very much also better positioned to look at national and international coordination or in the area of information exchange. The core, as I mentioned or the role of the FIU, is to detect, investigate suspicious transactions of clients and customers of the whole spectrum of financial institutions and I tell you what our scope is in a while.

On a more broader sense and teaming up with the objectives of the Reserve Bank of Fiji, the FIU has also a dual mandate of maintaining the safety and integrity of Fiji's financial system and that is the huge responsibility on us.

In the whole spectrum of things, we will ensure that foreign investors, local businesses, ordinary Fijians are protected from illicit financial flows including the harms of cybercrime. So that is who we are in a nutshell and that is what we do. Given our scope, mandate, role, functions are so broad and wide, our team is a bit small. We have a complement of nine permanent staff and three seconded staff. These seconded staff come from our partner agencies: the Fiji Police Force, the Revenue and Customs Tax and Revenue and Customs Office so they are full time based with FIU and this is how we manage our functions and our role.

You would have seen a lot of definitions of what constitutes the financial institution. In the FIU's context the financial institution is a whole spectrum of financial institutions not just licensed institutions like the RBF but includes non-licensed institutions like lawyers, accountants, real estate agents who provide any form of financial product and services, they are covered under the ambit of the Financial Transactions Reporting (FTR) Act and they are very much part and parcel of our umbrella of things that we do including preventative measures. The things that apply to a foreign exchange deal with a commercial bank also apply to anyone that is covered under the FTR Act.

This is a summary of what we do at the FIU. We disseminated 174 case dissemination reports or intelligence products to our law enforcement partner agencies on 259 individuals and 17 entities. We provided direct investigative assistance to 82 ongoing investigations on 195 individuals and 59 entities last year. We provided financial data reports on 113 cases involving 251 individuals and 229 entities, as I mentioned earlier, credibility checks and also foreign or international networking and co-ordination. Altogether, 418 intelligence products of the FIU disseminated to relevant agencies last year involving almost a thousand individuals and almost 400 businesses and entities. It is a huge role and burden on FIU to ensure that the financial system is clean, people who conduct financial transactions are adequately screened and our ordinary businesses and citizens are protected.

When we talk of dollar value over the last five years, our disseminations totalled around \$600 million of illicit or suspected illicit financial flows going through our financial system. These are the things that we see from the reported cases to us from the financial institutions and it could be more or less. This is just the suspected tainted proceeds, the actual cases would be determined by the law enforcement partners or the Office of the DPP when cases go before the courts. This is just what we are looking at each year.

The FIU continues to receive several cases on cybercrime itself and this involves internet banking, ATM scheming, email spoofing, business email compromised, phishing, spear phishing, identity theft and social media scams. If we have time at the end of the slide presentation, we can talk about some of these case studies and Esther can talk about one particular case study where certain individuals from a certain community in Fiji were subject to cyber scam. We would be happy to do that.

We are at a stage where the Committee is looking at the Cybercrime Convention (Budapest Convention) but I just wanted to brief the Committee that the work had started in 2010 and this is the involvement of the FIU. This goes back many years and FIU is one agency that was always in the loop, was always being consulted and we felt very humbled to be part of the whole programme of events that has translated over the last decade or so where we are at the stage now to sign the Budapest Convention.

I will not go into detail on all of these but just to emphasise to the Committee Members that FIU has contributed quite substantially to the drafting, framing of the Cybercrime Bill when it was being done. I think there were more than 10 drafts that the FIU had contributed and ensuring that all the elements, ingredients and requirements of the Convention were engrained and put in the cybercrime laws. We are confident that the Cybercrime Bill (now Act) that you had endorsed includes all the elements of the Cybercrime Convention.

On an international front, the FIU is well connected with the international partners. There are 166 financial intelligence units around the world that the FIU is connected and then we have got regional agencies such as the Pacific Cyber Security Operational Network (PaCSON) and Offensive Security Exploit Developer (OSED) that we also link up with in, in terms of raiding and preparing ourselves for the implementation of the Convention itself. So a lot of work has already been put in place and now we are at a stage where we can just go onto the next step of implementation.

Something I wanted to emphasise to the Committee that under the Budapest Convention, under international co-ordination and information exchange platform, there is a requirement that countries establish a dedicated 24/7 network channel with a dedicated team that is able to communicate and receive information and do certain things to protect and preserve electronic evidence.

Committee Members, the FIU became or is now the ad hoc G7 24/7 primary liaison point since 2018 but this is not part of the Budapest Convention outcomes but this is something that is running parallel and currently we have more than 90 members that are part of this G7 24/7 network.

I have a lot of slides but I will skip some of these but these are some of the things that we ensure that financial institutions are matching the mandate, the function and the role of the FIU to what we have been doing over the years.

The engagement with financial institutions is crucial so that when you and I, when our ordinary Fijians go before a foreign exchange dealer or commercial bank to conduct a transaction, they are adequately trained and our team is ready to receive reports and deal with them. At the moment, as we speak, there is a black list of foreign individuals whom the foreign exchange dealers and commercial banks cannot deal with because they are on the cyber black list issued by the FIU. These are some of the preventative measures that we have already put in place.

As you can see we have had a lot of cybercrime actual cases that we have encountered ranging from hacking, email scam, cybercrime, email spoofing, ATM skimming, Facebook scam and other scams. I will skip most of these, I guess other presenters would have done a fair bit of explaining to the Standing Committee on the ingredients of cyber security and cybercrime, but I will leave this as part of our submission so that there is a complete submission and the areas that we have included, include some of the key aspects of the philosophy behind the Convention and where we come in the picture as a country contributing to and supporting the Convention.

Business Email Compromise (BEC), if we have time, Mr. Chairman, Esther will take you through a BEC case and some statistics to warn and caution viewers about the extent to which Fijians can lose as a result of new cybercrime typologies that we have seen.

Are we ready for ransomware attacks? What are the consequences of a severe ransomware attack should it happen here in Fiji? I have got one recommendation for that and I will keep it to that. We have had some incidences of malware attacks, but if there is a full blown malware attack orchestrated by foreign cyber criminals, are we ready at policy, institutional and operational level to handle the side effects of any malware and ransomware attacks. We already have a good stakeholder framework which we have identified, we thought we will share with you in this submission. So we have a whole spectrum of regional institutions plus our own financial services and Telco service providers, including the academia and then we have the government agencies and then we have agencies such as the Ministry of Communications as the lead agency so to say in Fiji and then we have the Fiji Police Force, the Ministry of Defence, National Security and Policing, the FIU, the RBF, FICAC, Office of the Director of Public Prosecutions (DPP) and Office of the Solicitor-General and other agencies that join heads together to look at cyber security in the development of the cyber security strategy.

Articles 2 to 8 and 10 of the Convention talk about the things that we handle on a daily basis and we will be discussing with you some of the case studies that impact directly on the Convention, and you can make some recommendations as a result of the case studies that we will be discussing with you on Internet Banking Fraud (which is the direct component of the Convention), ATM Skimming, Email Spoofing, Business Email Compromise, Phishing or Spear Phishing, Identity Theft and Social Media Scams.

Let me conclude before we go on to the case studies. The FIU fully supports the proposed Convention on Cybercrime as it addresses the key gaps that we have seen so far in our daily operational areas in relation to cybercrime offences under the current Fijian Government's legal framework that includes the offences under the Crime Act, the Proceeds of Crime Act, the Financial Transactions Reporting Act and the Cybercrime Law.

The gaps in the government cybercrime regulations controls allow opportunities for cybercriminals to see Fiji as a potential haven to commit cybercrimes and exploit Fiji's financial systems and we are making very serious comments in relation to this because we are an agency that looks at cybercrime incidents on the ground at intelligence at operational, at investigation levels and also we have put in a lot of preventative measures, so when we talk about the case studies, I hope this comment will make a lot of sense to the Committee Members and it will also reflect on how much value we give to conventions on cybercrime and related areas including the Convention on Transnational Organised Crime and other related conventions. So I will go through some of the case studies (and Esther, how much time do we have, Chair. 15 minutes, okay).

Some of these case studies are related to cybercrime, some are not, this is just to give the context of the FIU and the readiness of Fiji as a whole, as a country, as a whole spectrum of agencies and institutions.

A 44-year-old man was reported to the FIU for conducting deposit transactions amounting to \$2 million in a three-year period. We established that he had \$4.4 million in investments and bank accounts. The individual was a director of two local companies. Bank account analysis showed that the funds in the investment and bank accounts were sourced from businesses with various narrations such as profit from business. We identified a discrepancy of \$8.2 million between deposits observed through his business and the amount that he declared for taxation purposes.

In 2020 a nightclub deposited \$30,000 in cash that triggered a suspicious transaction report from a reporting institution. The owner operates a nightclub as a sole proprietorship. In 2020 and 2021 (and you have guessed it right) in both those years we had a lockdown and an industry, a sector that was under longer lockdown period were the nightclubs. In 2020 and 2021, a nightclub received \$3.9 million in large cash deposits. It is unclear how the nightclub generated these funds given the COVID-19 restrictions that were in place in 2020 and 2021.

Another case study – a 26-year-old was receiving large cash deposits into his bank account totalling more than half-a-million dollars in a three-year period. The deposits were apparently from farm income. He also owned a freehold property. Spending patterns through the intel that we developed, his bank accounts indicated that he lived in a different area from where the alleged farm was located. Cash deposits were also done by third parties, a power of attorney was over the account for this one particular individual. There were other three individuals who were identified as having similar patterns in their bank accounts. They had conducted large cash deposits of \$5 million in three years and had acquired various freehold properties. You would have seen and heard about these particular case studies and these are just synopsis of the case studies that we wanted to put before the Standing Committee.

An individual on Social Pension Scheme had 37 land titles registered under his name.

A foreigner on a visitor's permit was found in possession of prohibited sea products. He owned three motor vehicles and paid his fine with cash. He does not have any bank account and it is unclear how he paid his fines or acquired his vehicles or other assets. A minor received an international remittance of \$150,000 from a foreign entity. You can make guesses as to what the minor was receiving from an offshore entity. An individual received multiple high value international money transfers from unknown third parties in a span of nine days.

In five months an individual received multiple deposits from third parties totalling a quarter-million dollars.

A person brought \$40,000 in cash as deposit to purchase property. The funds were not obtained from any bank account as far as our intelligence and investigation went.

A massage parlour received over half-a-million dollars in cash deposits followed by subsequent cheque withdrawals over a 12-month period.

An individual purchased an investment product with \$150,000 in cash.

An individual opened a bank account and in a span of two months he made 20 cash deposits ranging from \$9,200 to \$9,900 totalling approximately \$200,000. As you would know, Committee Members, that the current reporting threshold is \$10,000 which you honourable Members have supported and the threshold will now be reduced to \$5,000 from 1<sup>st</sup> of November.

An individual received high-value transfers of more than \$400,000 followed by ATM withdrawals and cash withdrawals of more than \$200,000 in two months. An individual deposited \$105,000 in cash into her personal account the notes were in \$100 denominations, the notes were sticky and moldy. A foreign national attempted to purchase a property with more than \$200,000 in cash. An individual would conduct monthly deposits into his four children's accounts collectively. He would deposit around \$10,000 to \$20,000 monthly, he withdrew \$300,000 collectively from the accounts and transferred the funds to another bank account and these are typical money laundering methods that anyone would do.

A public service officer acquired four taxi permits without paying for it. He and his wife collectively own four high value vehicles. He owns a freehold property in the Central Division and made significant improvements in the past few years, they frequently travel with the whole family and the children attend private schools. The individuals' transactions and accumulation wealth were not consistent with the annual income declared by this particular public servant.

An individual conducted multiple transfers to other individuals. The total cash and cheque deposits amounted to almost a million dollars in one year, the source of the bank deposits could not be determined by the FIU.

Politically exposed person (meaning you and myself are included in the definition) deposited \$17,000 cash into his personal account believed to be business proceeds. An individual received \$140,000 remittance in one month. She claimed to be from her brother-in-law to build a house. The sender was also remitting funds to certain person of interest that we were profiling, could be for drugs, cyber et cetera to a law enforcement agency.

An individual working at a financial institution provided a loan of \$1.5 million to an entity. A middleaged female in the United States sends several remittances within a few months totaling \$1.2 million to several young females in the Western Division. Maybe I will just hand over to Ms. Esther Sue to take us through some more case studies and in particular focus on the two cyber case studies on business email compromise and the one that I talked about that there were cybercrime victims from a particular locality and these are ordinary women who were involved in cybercrime transactions.

MS. E. SUE.- Thank you honourable Members. I shall start off with the business email compromise scam that the Director has mentioned. This is just a brief overview of how the scam works and then I will share some statistics in regards to how many cases we have seen and how much money that we have seen lost to this particular type of scheme.

In normal instances what we see is that the cybercriminal has been foreign. What the cybercriminal does is, they bypass internal firewalls et cetera of various companies to try and access some type of information. Now, sometimes they do this by phishing attacks where they can identify names or personal information to try and find out passwords et cetera.

Once they are able to gain access and sometimes it is through specific emails that have malware et cetera they hack that email account, the individual does not know, the entity does not know and they start accessing their emails and then they start liaising with the individual's suppliers, stakeholders et cetera.

In instances we have seen they will either purport to be the accountant or the chief executive officer and they will start exchanging emails with the regular supplier. They will create potentially an email address that might be quite similar you will see the original one at the top has got chief manager @live.com.fj and this one here says chief manager @live, sometimes it is actually very slight changes to the email addresses sometimes they get full control over the email addresses. It really depends, there are different strategies that they use.

They will then send a payment instruction to the Accountant and normally what they do is they send it in very odd hours of the day say 2 am or 3 am in a day. They will also change the normal format of those emails and they will tell them that something has happened to the previous account and that they need to urgently send the funds to a new account and the instructions are sent to be wired. Sometimes what they do is they also restrict access of the business to the original and correct email address. They do not know what is going on and they will ask them to send the funds. This is done to businesses, law firms as well as individuals. We see incidents of it may be two or three times a year but they are high value amounts.

The supplier will then send the funds to the foreign bank account. As you can see in that as soon as the money hits the foreign bank account it is immediately transferred to other accounts. This is not something that is just seen in Fiji it is something that is happening globally as well and even International Criminal Police Organisation (INTERPOL) has actually had campaigns around business email compromise as well.

Sometimes when the funds move to the foreign jurisdiction it does not just get split to two or three accounts within that foreign jurisdiction it actually moves to another country as well which makes it very difficult to trace and with remittances as well once they are following up with the supply it can be two to three weeks and at which point the funds have already left that bank account they sent it to and potentially also left that country. The cybercriminal then takes off with the funds.

In terms of statistics from 2016 to 2022 we have seen about 32 incidents targeting 27 entities and five individuals about more than \$6.4 million loss by the businesses and the individuals during that particular time. We have had may be one or two instances when there has been a partial return of the funds that was able to be sent by the entity or individual here and that was also because they picked it up quite fast when they asked for the recall of the funds from their bank and there were funds still available there.

A challenge as well is that, these business accounts and personal accounts that are established overseas are also receiving funds from all over the place because they are also trying to deceive other individuals trying to differentiate who those funds belong to when it is a small portion and they have stolen a certain amount from different countries is also a challenge for those entities and jurisdictions.

The top three destinations in terms of funds that we have seen go out of the country resulting in this kind of scam is Hong Kong, USA and Australia during this period.

Something that we normally advise entities and members of the public is if there is any change in a payment instruction to exercise extreme caution with that. We advise as well that if there is a phone contact of the suppliers that they have been dealing with or the individuals that they have been dealing with for them to call them to verify that that particular change is correct. Sometimes what we have seen is the change in the account that they have proposed, the name of the account is actually quite different from the name of the business that they are actually dealing with et cetera. Just ask questions with the suppliers of the individuals they are dealing with and try and protect themselves from being victims to the scams.

In 2022 within January February (that is where we saw the cases this year) there was more than \$400,000 lost, they were two local businesses. They do target the businesses because to be able to get this type of money you would have to target the businesses.

I would like to talk about that which targets actual individuals. It is a cyber loan scam and it had targeted a specific community within Fiji. It was between December 2019 and April 2020 and we found that there were 73 Fijians in that particular community that conducted 163 remittances to 41 individuals in Benin - they sent around \$98,658. What happened was there was an individual that was purporting to provide loans to them and the victims were paying around \$395. Some were like \$50 but I think most of it was around \$300 to \$400 to that particular individual and then that individual would send the funds onto the scammers in Benin.

You will see in there we call them money mules. Generally when we are looking at scammers they will have to I guess, for lack of a better word, they will have two cons: that with the victim where they will offer them a loan potentially and then the second is with the money mules. Potentially they will say that it is an online job saying we are going to send you a set amount of money, you keep a certain amount and then you send the rest to us. They could say that we want you to test the customer service for that particular agency we want you to send the funds to and et cetera. They are quite sophisticated and there are different stories that they tell to different individuals to get the funds to move. Because of the exchange control restrictions that we have as well within Fiji for remitting funds out, that is why you see a high number of remittances and they try and split it, they are aware of these exchange control restrictions. They know what amounts to ask for and they are very aware of all the different restrictions that we have in place and how to potentially bypass it et cetera. I think that is all from me, I just hand back to Director. Thank you.

MR. R. BUKSH.- Thank you, Esther, those are some of the case studies that we have seen. We are in Fiji at a mode where we call it a “reactive mode” where we react to incidents. The FIU is slightly 1.5 ahead in the equation. We are reactive plus preventative as well. We put in place adequate measures so that Fiji does not continue to fall victim, for example no person in Fiji or business in Fiji can send any remittance to a person in Benin without seeking approval of the FIU because of the high risk that we have seen Fijians become victim to this.

Mr. Chairman and honourable Members I will skip some of the slides and just go on to the last bit and this is where we fit in. We ensure that the whole of Fiji including Fijians and Financial systems remain protected from the harms of financial crimes including cybercrime.

We have a lot of responsibilities on our shoulders including ensuring the compliance by Fiji on international standards including compliance with the Budapest Convention, Convention on Cybercrime - there is a huge responsibility. When you see 100 percent compliance with international AML/CFT standards, the Cybercrime Convention has got direct impact on the role of the FIU as you have seen in the various case studies and the role and functions of the FIU.

With those submissions, Mr. Chairman and honourable Members of the Standing Committee, we fully support Fiji's position in terms of ratifications, signing and implementation of the Budapest Convention as soon as possible and FIU stands ready to provide any support that may be needed by the Fijian Government and its line agencies so that we can fast track some of the reforms including the handing over of our role as the current G7 24/7 network liaison point and having strong partnerships with agencies that will be formed under the Budapest Convention including the possible role of the FIU in the Fiji set and also in the taskforce that we look at the whole spectrum, whole wider things that will come as a result of the various requirements and the Articles of the Budapest Convention. Thank you and vinaka vakalevu.

MR. CHAIRMAN.- Thank you, Mr. Buksh and the team for that very comprehensive brief but very comprehensive and also giving us an insight into the case studies. It is an eye opener for us the subject matter itself. Are there any questions, honourable Members? Honourable Dr. Govind?

HON. DR. S.R. GOVIND.- Mr. Chairman, thank you for a very knowledgeable presentation. I am just wondering you have such a small number of staff and looks like Esther is the only person who is knowledgeable about keeping the surveillance going. How do you handle that with minimal staff and technology 24 hours - all these things seem to be very enormous task.

MR. R. BUKSH.- Thank you, honourable Member you are absolutely right. These are the concerns that the FIU has been raising all along but we do not shy away from doing our job despite resource constraints so we are fully supported and backed by my two very knowledgeable people: on my left who complement the work of the intelligence team and they are the IT. At present we have 21 million or over 21 million financial transactions in our database. That include suspicious transaction reports, remittance reports whether it is coming from Western Union type of agencies or from a commercial bank, FX dealer transactions or it is border currency declarations or even cash transaction reports. The IT team ensures that there are sufficient rules that pick up any indicators ready for the Intelligence to make some sense and issue these reports to the relevant partner agencies. Yes, I totally agree that we have resource-constraints in terms of human resources but we capitalise on our IT support. We have 24/7 certain rules that pick on transactions that are happening with any of the reporting institutions and it will give reports to the Intelligence team.

Together with that, they have a very sophisticated search functionality and the Australian Government through the Australian Financial Intelligence Unit has just provided us with technical assistance by enhancing our software called "TAIPAN". That system will further allow our Intelligence team, without much human resources to do data mining and visualisation of key financial data to use that will be used by our partner agencies.

So we do it through technical means and this is where this Convention becomes so relevant to us that when we have connections with the private sector, when we have connections with the law enforcements partners, we must ensure that the online communication mechanism is done under certain protocols and this Convention, we hope through

the establishment of the taskforce as a result of this Convention will set those protocols, will set those rules so that when Esther and Lawrence and FIU are able to communicate, we are able to do it on a very secure and protected platform. I am not saying it is not secure but we have certain standards that will regulate the security of communication and information that is held.

HON. DR. S.R. GOVIND.- She was showing us the surveillance thing, how people are transferring money through different businesses. Does that require like physical presence to watch and follow or when you are away from office, who does that or you watch from home? How do you manage the surveillance system?

MS. E. SUE.- We have certain rules that are built within the database itself and we have certain reports. We call them indicators. There are some that we receive directly from our reporting entities but for certain situations if we are trying to monitor, we will set rules on the system and then we get email notifications. The Intelligence team is not just me, there are actually six of us. I lead the team, Sharlene is one of our analysts and then we have four more back in the office including our seconded officers. The Director is also copied in it. At any point when someone is not away, there is someone acting to take on that particular position and certain management of that. We have certain SOPs that we abide by as well in terms of how we record, reports are coming in and how we monitor it, et cetera. We do rely heavily on technology to generate those reports and then to flag it to a few of us and there are specific people identified to look at individual reports.

HON. DR. S.R. GOVIND.- The final question is that, with certain countries with regards to Benin, which of these countries can you not send remittance to?

MS. E. SUE.- If I could just clarify: with the remittances for Benin, it is not so much as a blanket, we cannot send remittances to Benin, we have identified that being potentially a country where people are sending money, could be victim of scams. So we have advised the reporting entities of financial institutions to just ask a bit more questions. Just telling them that these particular countries, they could be victims of scams if they are sending money there. They will ask certain questions and if they identify after asking questions to the customers that it could be a scam, they will advise the customers as such. In some instances if the customers still choose to send those funds, they may refer the customers to us to have that conversation with them to try and convince them not to send the funds abroad. It is not a direct blanket, I guess, restriction on those particular country but there are individuals we have identified who have been receiving funds from victims in Fiji and we have asked those reporting entities or financial institutions to not send funds to those individuals.

HON. P.W. VOSANIBULA.- Mr. Chairman, there are millions of transaction information with you, if there is a cyber-attack, what remedial action do you have in place to deal with those attacks on such transaction information?

MR. R. BUKSH.- Firstly, all the 99.9 percent of our reports reported by reporting entities to the FIU is done on an encrypted format, if the file is intercepted by any malware, the file remains protected because it is encrypted. The 21 million financial transaction information in our database is controlled or secured in a very secure platform and then we have several firewalls and protocols and these are consistent with the international security protocols. We use the hardware or the entire IT infrastructure of the RBF, we are no different in terms of our IT backups so we have a business resumption site as well where we can close certain ports and we will be able to still carry out our operations on a daily basis. We operate on a very secure platform but currently these security platforms and protocols are determined by the FIU and the RBF.

Under the cybercrime Convention and the necessary structures that will be established under the Convention, the Ministry or Body will be able to then dictate what would be some of the standards that Fijian agencies should need to deploy to protect, honourable Member, the type of question that you ask, exactly this Convention has a direct impact on the question that you posed.

MR. CHAIRMAN.- If there are no further questions, I take this opportunity to say thank you Mr. Buksh to you and your team for availing yourselves this afternoon. Should we have any other questions at a later date that you will avail yourself to answer those questions or come before us again. With those few words I thank you and if you have any departing remarks the floor is yours.

MR. BUKSH.- Mr. Chairman and Honourable Members thank you and my apologies for taking a bit more time. Yes, this is a very relevant and important step that Fiji should undertake more seriously and prioritise some of the implementation measures. The FIU as I have mentioned in my submission stands ready to provide any support and networking that would be needed in the implementation phase of this particular Convention. Thank you very much and vinaka.

MR. CHAIRMAN.- Thank you.

The Meeting adjourned at 12.08 p.m.

**Interviewee/Submittee:** Citizens Constitutional Forum (CCF):

**In Attendance:**

- |                       |   |                                |
|-----------------------|---|--------------------------------|
| 1) Louchrisha Hussain | : | Chief Executive Officer (CCF); |
| 2) Milika Ligabalavu  | : | Policy and Research Officer;   |
| 3) Ms. Lusia Lagilevu | : | Programme Manager              |

MR. CHAIRMAN.- Honourable Members; members of the public; secretariat; ladies and gentlemen: a very good afternoon to you all and it is a pleasure to welcome everyone especially the viewers that are watching this proceeding.

For your information pursuant to Standing Order 111 of the Standing Orders of Parliament all Committee meetings are to be open to the public therefore please note that this submission is open to the public and media and is also being screened live on Parliament's Website and social media online platforms and the Parliament Channel on the Walesi Platform.

For any sensitive information concerning the matter before us this afternoon that cannot be disclosed in public this can be provided to the Committee either in private or in writing. Please be advised that pursuant to Standing Order 111(2) there are only a few specific circumstances that allow for non-disclosure and these include: national security matters; third party confidential information; personnel or human resource matters and Committee deliberation and development of Committee's recommendation and reports.

I wish to remind Honourable Members and our guests that all questions to be asked to be addressed through the Chair. This is a Parliamentary meeting and all information gathered is covered under the Parliamentary Powers and Privileges Act. Please bear in mind that we do not condone slander or libel of any sort and any information brought before this Committee should be based on facts.

In terms of the protocol of this Committee meeting please minimise the usage of mobile phones and all mobile phones to be on silent mode while the meeting is in progress.

Allow me now to introduce Members of my Committee

(Mr. Chairman introduces Committee Members; Committee Secretariat and Hansard Staff)

Today the Committee will be hearing a submission on the Convention on Cybercrime otherwise known as the Budapest Convention. For the purpose of the viewers that are joining us this afternoon allow me to give a brief explanation of the Treaty.

The Convention on Cybercrime also known as the Budapest Convention provides a comprehensive and coherent framework on cybercrime offences and electronic evidence. It serves as a guideline for any State developing

comprehensive national legislation against cybercrime and as a framework for international cooperation amongst State Parties. To date the Convention has 67 member States which include Australia and Tonga from the South Pacific region.

Pursuant to Article 37 of the Convention, any other State such as Fiji can become a Party by accession if the State is prepared to implement the provisions of the Convention and upon invitation to accede to the Convention after consultation and approval of parties.

With the extreme effects of global cyber threats and attacks on critical sectors such as finance, ICT, energy, water, emergency services, public safety, health, public services, aviation and e-government infrastructure, becoming a party to the Convention will enhance Fiji's ability to combat cybercrime with international support and assistance particularly in relation to continuing capacity building to better equip

Fiji's criminal justice authorities including the judiciary, prosecution and law enforcement agencies.

Ladies and gentlemen, before us this afternoon we have the Citizens Constitutional Forum ably led by their Chief Executive Officer Ms. Hussein and I give you the floor Ma'am to introduce your team and do your presentation after which we will have a question and answer session. Thank you and the floor is yours, Ma'am.

MS. L. HUSSAIN.- Thank you Mr. Chair for the welcome. I am Louchrisha Hussain the Chief Executive Officer of the Citizens Constitutional Forum; and to my right is Ms. Milika Ligabalavu our Policy and Research Officer; and further to her right is our Programme Manager Ms. Lusia Lagilevu. Ms. Ligabalavu will be addressing the Committee today and if you will allow during the question and answer session Ms. Lusia Lagilevu and I will also address the questions. *Vinaka.*

MS. M. LIGABALAVU.- The Chairperson (honourable Alexander O'Connor) and honourable Members of the Parliamentary Standing Committee on Foreign Affairs and Defence: a very good afternoon to you all.

The CCF thanks the Standing Committee for the opportunity to provide a submission on the Convention on Cybercrime also known as the Budapest Convention and referred to as the Convention. The CCF is a non-governmental organisation based in Suva with over 20 years' experience in education and advocacy on human rights, democracy, good governance, transparency and accountability, rights as reflected in the Bill of Rights in Fiji's 2013 Constitution and multiculturalism.

The CCF acknowledges the purpose and positive impact of becoming a party to the Convention, however, there are a number of recommendations that the CCF believes need highlighting before becoming a party to the Convention.

I will now proceed to discuss the key points on the Convention on cybercrime and I begin with the first key point which is the definition of fundamental human rights.

Freedom of expression and right to privacy are fundamental human rights that are recognised under the 2013 Constitution of the Republic of Fiji and the ratified international conventions.

Section 24 of the 2013 Constitution of the Republic of Fiji provides for the right to privacy which includes confidentiality of personal information, confidentiality of communications and respect for private and family life.

Article 15 of the Convention requires parties to uphold the protection of human rights under domestic laws and international conventions such as the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms. Section 24 of the 2013 Constitution of the Republic of Fiji provides for the right to privacy which includes confidentiality of personal information, confidentiality of communications and respect for private and family life.

Article 15 of the Convention requires parties to uphold the protection of human rights under domestic laws and international conventions such as the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms and the United Nations International Convention on Civil and Political Rights (ICCPR). Fiji is a party to the ICCPR.

The definition and recognition of the right to privacy is stated in Article 17 of the ICCPR and Article 8 of the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms. Freedom of expression is covered under Article 19 of the ICCPR and Article 10 under the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms. While these fundamental rights are defined and recognized under the two international instruments, Citizens' Constitutional Forum (CCF) notes that these definitions are not specifically defined within the context of cybercrime that is, there is no specific definition for privacy and what constitutes freedom of expression.

The CCF also notes that the current domestic legislation, the Cybercrime Act 2021 does not define these terms. Ambiguous cybercrime laws can give rise to its abuse as the interpretation of its provisions will be dependent on those who are enforcing it.

The second key point - Balancing Human Rights and the Power of National Security: limitations to any human right must be done so in accordance with the principle of proportionality. This is also stated in Article 15 of the Convention. The principle of proportionality requires that any interference of rights must be proportionate with the legitimate reason for limiting it. Furthermore, matters of public interest change over time due to technological developments and societal attitudes.

The CCF submits that knowing what constitutes public interest within a law is essential in protecting human rights as well as ensuring good governance, transparency and accountability of the State and law enforcement agencies. The CCF submits that proper safeguards must be incorporated to ensure that acts or information which invades or restricts the right to privacy and freedom of expression without legitimate cause and proportionality does not take place. This should also be done in domestic legislation without delay. The CCF urges government to be mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the United Nations International Covenant on Civil and Political Rights (ICCPR) and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy.

We therefore submit several recommendations to the Standing Committee;-

- a. There must be specific definitions of privacy and freedom of expression within the context of cybercrime. Domestic legislation such as the Cybercrimes Act 2021 needs to be reviewed to define privacy as well as state what constitutes freedom of expression and public interest;
- b. Proper safeguards be incorporated into the Convention and domestic legislation to protect fundamental human rights, avoid its misuse and encourage transparency and accountability;
- c. The need for guiding principles for the appropriate and accurate application and implementation of the same to ensure that citizens' fundamental human rights and freedoms which are enshrined in Fiji's 2013 Constitution are not violated;
- d. Government to prioritize inclusive public consultations, given Fiji's diversity. Conducting meaningful engagement and collaborative work with local communities, civil society organisations and a wide range of stakeholders in addressing societal and cultural norms that pose barriers is needed during national processes of drafting and implementation of new policies and laws; and finally
- e. Monitoring, development and/or revision of frameworks in support of the implementation of the Convention (subject to the protection of human rights) and any relevant recommendations received from state and non-state actors must be genuinely considered and reflected locally without impractical delay. Thank you.

MR. CHAIRMAN.- Thank you Ms. Ligabalavu for your presentation and that of the Citizens' Constitutional Forum. You have proposed some recommendations for us which are very good insofar as the Committee is concerned and we will take that into consideration when we deliberate over the report writing. Honourable Members, any questions for the CCF team?

HON. L.S. QEREQERETABUA.- Mr. Chairman, Sir, just to say thank you very much ladies for your presentation. You have proposed some recommendations for us which is very good insofar as the Committee is concerned and we will take that when we deliberate over the report writing. Honourable Members, any questions or comments for the CCF team?

HON. L.S. QEREQERETABUA.- If I may, Mr. Chair, through you, just to say thank you very much ladies for your presentation. I know the Committee has heard a few submittees and the different recommendations and I just want to say thank you very much for especially raising the red flags on human rights.

---

MR. CHAIRMAN.- Now, honourable Members, I take this opportunity again, CEO and the team for availing yourselves this morning. We are sorry for the inconvenience in the slight delay in your presentation but we look forward to avail yourselves should we have that need to be able to consult your good selves again.

With those few words a blessed afternoon. If you have any departing comments the floor is yours, thanks Madam.

MS. L. HUSSAIN.- Thank you Mr. Chairman. We just want to take this opportunity to once again thank the Committee for hearing our submission *vinaka*.

MR. CHAIRMAN.- Vinaka thank you.

The Committee adjourned at 12.36 p.m.

# **[VERBATIM REPORT]**

## **STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE**

### **Convention On Cybercrime**

**SUBMISSIONS:** (1) Ms. Salanieta Tawanikaiwaimaro  
(2) Datec Fiji Limited  
(3) Fiji Police Force  
(4) Fiji Human Rights and Anti-Discrimination Commission

**VENUE:** Small Committee Room, Parliament

**Tuesday, 4<sup>th</sup> October, 2022**

**DATE:**

**VERBATIM REPORT OF THE MEETING OF THE STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE  
HELD AT THE SMALL COMMITTEE ROOM (WEST WING), PARLIAMENT PRECINCTS, GOVERNMENT  
BUILDINGS, ON  
TUESDAY, 4<sup>TH</sup> OCTOBER, 2022 AT 9.30 A.M.**

Interviewee/Submittee: Ms. Salanieta Tamanikaiwaimaro

---

MR. CHAIRMAN.- Honourable Members, members of the public, the secretariat, ladies and gentlemen, a very good morning to you all and it is a pleasure to welcome everyone especially the viewers that are watching these proceedings. For your information, pursuant to Standing Order 111 of the Standing Orders of Parliament, all Committee meetings are open to the public, therefore, please note that this submission is open to the public and media, and is also being streamed live on Parliament's website and social media online platforms, and the Parliament channel on the Walesi platform. For any sensitive information concerning the matter before us this morning that cannot be disclosed in public, this can be provided to the Committee either in private or in writing.

Please, be advised that pursuant to Standing Order 111(2), there are only a few specific circumstances that allow for non-disclosure and these include:

1. National security matters;
2. Third party confidential information;
3. Personnel or human resources matters; and
4. Committee deliberation and development of Committee's recommendation and reports.

I wish to remind honourable Members and our guests that all questions to be asked are to be addressed through the Chair. This is a parliamentary meeting and all information gathered is covered under the Parliamentary Powers and Privileges Act. Please bear in mind that we do not condone slander or libel of any sort and any information brought before this Committee should be based on facts. In terms of the protocol

of this Committee meeting, please minimise the usage of mobile phones and all mobile phones to be on silent mode while the meeting is in progress. Allow me now introduce the Members of my Committee.

(Introduction of honourable Members of the Committee)

Today, the Committee will be hearing a submission on the Convention on Cybercrime otherwise known as the Budapest Convention. For the purpose of the viewers that are joining us this morning, allow me to give a brief explanation on the Treaty.

The Convention on Cybercrime, also known as the Budapest Convention provides a comprehensive and coherent framework on cybercrime offences and electronic evidence. It serves as a guideline for any State developing comprehensive national legislation against cybercrime and as a framework for international cooperation amongst States Parties. To date, the Convention has 67 members which includes Australia and Tonga from the South Pacific Region. Pursuant to Article 37 of the Convention, any other State, such as Fiji, can become a party by accession if the State is prepared to implement the provisions of the Convention and upon invitation to accede to the Convention after consultation and approval of Parties.

With the extreme effects of global cyber threats and attacks on critical sectors such as finance, ICT, energy, water, emergency services, public safety, health, public services, aviation and e-government infrastructure, becoming a party to the Convention will enhance Fiji's ability to combat cybercrime with the international support and assistance particularly in relation to continued capacity building to better equip Fiji's criminal justice authorities including the judiciary, prosecution and law enforcement agencies.

Ladies and gentlemen, before us this morning we have Ms. Salanieta Tamanikaiwaimaro joining us virtually online from London, Great Britain. I request Ms. Tamanikaiwaimaro to introduce herself and to begin her submission, after which there will be a question and answer session.

MS S.T. TAMANIKAIWAIMARO.- Members of the Standing Committee on Foreign Affairs and Defence - the Chairman, honourable Alexander O'Connor, the Deputy Chairman, honourable Dr. Salik Govind, honourable Selai Adimaitoga, honourable Peceli Vosanibola and honourable Lenora Qereqeretabua; thank you very much

for the invitation to join you. I would also like to thank the parliamentary support team for the excellent facilitation of the technology and support to enable ordinary people like us to be able to come and make our submissions.

First of all, I would like to express my deep and heartfelt gratitude to you all for the incredible work that you are all doing - serving the people of Fiji in your various capacities. It is not easy and before I begin my submission I want you to know that you are all amazing people - you are serving our beloved country Fiji, we love you so much and we are praying for you.

I seek leave Mr. Chairman, to begin my submission. First, of all I would like to say that I have been following the deliberations and the *Facebook* streaming and I thank the technical support team particularly the Parliamentary IT Department for facilitating and making it available to us. It is really wonderful just to hear the diverse views of different people and different organisation from all across Fiji.

Mr. Chairman, if I could introduce myself. As you know, my name is Salanieta Tudrau Tamanikaiwaimaro. I am from Naisausau, Namara, Tailevu *vasu* of Drekeniwai, Cakaudrove and my grandmother is from Moturiki but I have bloodlines all across the provinces. It is a privilege to address this august body but before I begin my submission, I was hearing everyone's comments on the law so I will not bore you with any of that. What I would like to address first of all is the categories of what I would like to highlight in my submission and if possible Sir, could I send my written submission later in the day to help you with your deliberations?

MR. CHAIRMAN.- Yes, Madam, much appreciated

MS. S.T. TAMANIKAIWAIMARO.- Thank you so much. Mr. Jacob very kindly sent me the Budapest Convention and the 137 pages Special Edition of the Budapest Convention. That was a very important document particularly the 2022 Special Edition because it historically puts into context the history of how that Treaty got negotiated.

As early as 1983, you would have read in the Special Edition that the OECD deliberated on how countries can harmonise their laws, particularly the international laws, for the purposes of facilitating their criminal

justice system or if someone was prosecuting or if they needed to investigate a particular matter. But as I said, let me take a step back and point out the four things that I would like to talk about today.

1. The context; because I believe context shapes meaning;
2. The international law; I will be sending you written submissions and the analysis where they have done the comparative law exercise;
3. The substantive domestic law which is the Cybercrimes Act itself; and
4. The capacity and readiness; basically, are we ready for it?

Mr. Chairman, those are the four things but firstly, I would like to talk about context. Personally, I have always felt that context shapes meaning. If you take a book and you take a sentence out of the book but if that sentence is not read in whole with the book, it can be misconstrued - does that kind of make sense. Take for example, the *Bible*. I am just using the Bible as an example because I am a *Christian*. If you are a *Hindu* you can use the *Mahabharata* or *Ramayana*, if you are Muslim you can use the *Quran* but because I am a Christian, allow me to use the *Bible*.

You can take a verse and interpret it, but to interpret that verse you would need to look at the pretext and the context of what that verse actually means. What is it trying to say? The law is pretty much similar and that is why I am saying that context shapes meaning - how did this law come to pass? How was it birthed?

It is very important to know what the Council of Europe and all the Parties to the Budapest Conventions celebrated at the 20<sup>th</sup> year anniversary. In other words, it has existed for a while, but if you look at the Special Edition Report and if you go through the 137 pages (and of course it is open to the public and that document is available online) you will see that the Budapest Special Report 2022 talks about the historical context of how that treaty was negotiated, as early as 1983 and going forward.

Now why is that important? It is important because at that time when the drafters drafted, they drafted using language like computer related offences and you can see that it still followed the residue. Imagine for example, a dress or something old like a fabric and then after 20 years you need to patch it - does it make sense? We need to patch it because there is a lot of wear and tear, the seasons come and go so obviously, as we have seen in the last decades, things have evolved like devices that we never thought would exist, exists

now. We have smart fridges and smart phones. Now someone can look at their security through their computer and there were people talking about difference devices - you have smart washing machines, almost everything we know that has become computerised, are smart, like the electric car, now we have autonomous cars and driver-less cars, and all sorts of things.

I wanted to discuss context because I would like to ask the Standing Committee to also consider the lay of the land when considering the context - not just the context of the international law and the history of it and we will go into the law later, but the lay of the land which is the people, the Government and the finances (the coffers), because at the end of the day everything boils down to the bottom line and public interest.

How will signing this Convention affect Fiji's bottom line? How will that affect global public interest or let us bring it down to the ordinary citizens of Fiji. That is what I was trying to say when I was talking about context, like the lenses to view the international instrument.

Let us take, for example, Convention 23.XI.2001 otherwise known as the Budapest

Convention. Remember the fabric that I talked about that it was good for that time and some consider it still good to some extent. So, if you look at the special document of 137 pages, it talks about when the negotiators were negotiating because obviously, countries were at loggerheads as to the offences they would like to put in. What they did was that they went for their minimum offences at that time which was the minimum in the 80's and 90's, does that make sense?

Chairman O'Connor posed a very good question to the Solicitor-General's Office when they were making their submissions. How did we do the law? Should we not have done the law after doing the Treaty? How did we get to do the domestic law before the Treaty? You actually nailed it, Sir, when you said that because it was like a back to front thing.

When I send you my submissions, I will send you a couple of documents which have already done the cross analysis - summaries of sections from the Cybercrime compared to the Budapest Convention - how they match and overlap, keeping in mind what I had said about context and the fabric. There were a lot of criticisms against the Budapest Convention but the reality is that there will always be criticism. Nothing is perfect in this

world but in terms of the Budapest Convention, there have been contentions in relation to the text. But obviously, the text was drafted at a time when computers were new, and things were new.

When you use the word “cyber” and I am going to speak very plainly because I recognise that I am not only speaking to the Standing Committee but also to the people of Fiji who are listening in - there is a big difference between cyber and computer. Computer is a device that exists within the cyber environment and this is where context comes in. With your permission, I am going to share a picture which I would like to explain to you. Basically, when we say the cyber environment, we are talking about three layers. One layer is the physical layer – you can imagine this layer as the base stations like the ones in Kadavu, Labasa or Taveuni – you will see a base station and that is how Digicel is able to catch. It looks like those big towers, or even around Suva you will see optic fibre cables - cables that are either copper or optic fibre, those are part of what is called telecommunications infrastructure; these are all physical layers – the telecommunications infrastructure, that is the first layer.

Then you have the second layer, which is what we call the transport layer. In this layer you will have the devices, the computers but you will have Transmission Control Protocol/ Internet Protocol (TCP/IP), Domain Name Server (DNS). Basically what it is, for example, if I want to go to the parliamentary website, I just type in the URL or the web link, so that is the transport layer. Then you have got the last and the third layer, which is the application layer, which is content and applications. Those are things like apps on your phone - Facebook.

You would have heard the Deputy Permanent Secretary of Ministry of Communications talking about double authentication. That is fancy language for saying that instead of me logging into my Facebook with just my password, this time they want to see my face - like biometrics. When they say two factor authentication, it is just fancy language for saying - okay two tests to verify that this is indeed Chairman, O'Connor, and not Jone Vukive. It even includes things like ATM machines. For example, you are on a plane and it is linked to the satellite and they are accessing coms, or the boats that are linked to satellite are accessing coms, so the satellite is the telecommunications infrastructure but the application is what the user is able to access.

Very quickly, just by showing you the picture of the three layers, you will see how even the language of computer related offences is a very thin spectrum. It does not even cover the word ‘cyber’. Remember, we

cannot really criticise the drafters. We have to congratulate them and thank them - they did amazing work because for that time and period in which they drafted it, it was valid for maybe 10 years or 20 years.

My personal view is they need to really review it in to factor in the state of play of the cyber environment as it exists today - that is the first thing. One of the things that Chairman O'Connor very cleverly pointed out was when he asked how did we do it back to front, and should we have done the Treaty before the law? When you receive the spreadsheet, you will see that much of the Convention is already in our domestic law. There are just a few pieces that are not in our domestic law, but the bulk of it. I have put it in my submission and you will see it will be in the form of an excel sheet to make your deliberations easy.

I would encourage that if you have a question on any of the aspects that I am saying, just make a note of it and then you can just ask me. So I have explained the cyber environment and the computer related offences without even going into the law right. Now, we are going to go into the law so esteemed Members of the Standing Committee, you are parliamentarians and you will know this. There is a hierarchy of laws that when push comes to shove, the way it gets interpreted by the judiciary is the hierarchy. I am trying to speak plain English so the ordinary members of the public will be able to follow as well.

You know how we play last card and we have the ace - the ace is more powerful and obviously, if you want to penalise you have the Jokers and things like that. Similarly, in the hierarchy of laws, we have got the Constitution which is like the trump (or in Fijian – *tarabu*) and the Constitution trumps every law. Second to that is the legislation from Parliament and obviously following that are decrees made by Cabinet and then the regulations and subsidiary legislation - why is that important? It is important because when deliberating on the issue of whether we sign up, we check the Constitution. What does the Constitution have to say about international law? What are our limitations? Can we do this? That is one way of looking at it.

I have taken you through a very brief historical overview of how the Budapest Convention was developed and I do not really need to get into that because it is covered by the special edition document. But essentially if you look at our Cybercrimes Act of 2021, and I will not bore you by going through all of it because I will send you the spreadsheet and it will show the sections, but pretty much let me say that 90 percent of our Cybercrimes Act already complies with the Budapest Convention, in terms of the offences. Like I said, only

two or three offences are not in our Act per se but in terms of things like issues of preservation of data or collecting evidence, it is almost like we have mirrored it. Again I am reiterating that we did it back to front.

I said this when I made submissions online on the Online Safety Bill at the time. We had talked about context as well and the importance of looking at all the other laws. One of the things lawyers tend to shortcut on is doing a proper mapping of everything that exists domestically. For example, the dress that fits honourable Lenora, I cannot assume it is going to fit me. In other words, the dress that fits the United States of America or that fits the Council of Europe, just because they shove money in my face or push stuff to me, I cannot assume that it is going to fit me.

We can snip here and patch-patch there but at some point when we do that, when we do not realise we have other things, in other words the dress that was made for the United States of America was made for the United States of America; what was made for Germany was made for Germany. What the Budapest Convention did and did successfully (and we have to congratulate them) was for harmonizing mutual cooperation. It was successfully done and we have got to congratulate them for that, but the issue is - will it fit me? Will it fit Fiji? Will it fit the lay of the land here in Fiji? Take for example Australia and I am going to share with you a paper that I wrote and published in 2011 called Cybersecurity in the Republic of Fiji where I did a comparison of laws for different countries. Even then you will see the different categories of offences.

Australia has different instruments criminalizing different things. America has different instruments criminalizing different things, but when they came to the Budapest Convention and people were negotiating the text, which you will see in the Special Edition, they negotiated on the agreed minimum offences at that time. I just want to ask you something - is there anyone wearing any clothes from the 1980s? No one. In the fashion sense, it is a trend and we want to be up with the time, everyone has changed, but in the context of cyber the environment has totally changed. Does this make sense?

It has been a blessing (not a curse) that we actually have not yet signed. They have had issues in Europe, in England, issues everywhere in relation to some of the things that we are talking about - the difficulties. The benefit of being a late comer to the situation is that you get to leapfrog. Does this makes sense? Yes, I just want to say that.

Back to the crux of it, I am going to point out the evolution of three legal international instruments. The first one is the Budapest Convention 2001 and decades later, they created the additional protocol on the Convention on Cybercrime concerning the criminalization of racist xenophobic content through computer systems - again, that is content-related offence. Then in 2003 was the Second Edition Protocol on Enhanced Cooperation and Disclosure of Electronic Evidence. This was what I meant by the old fabric and then the patchwork. As you make your deliberations you can discuss - do we sign this? Do we make reservations here? How far can we go? Does it mean that we have to go fully in, or do we hold back?

Going back to context - the lay of the land. I went through the government budgets from 2016 to 2021 and basically, the budget that I was trying to pull out was the Police budget. You will ask - why is this necessary? This goes to context - the lay of the land. If you look at the budgetary capacity, it is more or less the same, which speaks to me about capacity. This is the limit. It is very easy to say mutual cooperation but remember everything boils down to the bottom line and it costs money. Let us zoom in to who in the Police Force looks after cybercrime – it is the Cybercrime Unit. How many staff are in the Cybercrime Unit? What resources do they have? What forensic capacity do they have? If you look at the budget it is the same, more or less. I will screen-shot everything and send it to you.

Why is this important in this conversation? The reason is that when we sign a Treaty or when we ratify it, we become obliged. We become obliged obviously to cooperate. So, for example if the FBI through their Department of Justice serves the Solicitor-General's Office with notice to say "This is a production order, release this" and they send it to Digicel, or Telecom, or FINTEL or USP because USP manages .fj the country code top level domain. This is the production order, release this, I want to know this. Can you imagine - do we have the capacity? Let me just say (I cannot speak for the Police) but this is where your Committee comes in and you can certainly ask them - how is the load? How much does it cost?

Imagine if all these countries that have signed and ratified, start sending multiple production orders - can our system have the capacity? There is no issue with extradition because we already have the extradition laws in place that allows for mutual cooperation. We already have it in our domestic law. If we choose voluntarily to participate, yes, of course we can do that. It is already in our law. But signing up to an international instrument means you become legally bound. Obviously if you are unable to produce you will be able to say

that you are unable to produce, but does the Office of the Solicitor-General have the capacity to respond to an avalanche of production orders, should that time come?

The other thing I wanted to say is when they ask for cybercrime information it is time sensitive but internally in the country, can we say we already have a uniform time. My time here is 11.10 p.m. and your time is 10.05 a.m. Can we say that all across Digicel, Telecom and FINTEL it is 10.05 a.m. for one particular IP address because remember a milli-second difference is a different user. So would it not be better if we strengthened our core domestically and nationally as a country. We build our core. We have robust policies and framework like uniform timestamps and strengthen our own systems, such as the Police Force, or even the training of the Judges. We thank the Council of Europe for the amazing training they have been doing with our Judicial Officers and that is really important. But there has to come a time when we have to have a dedicated court for cyber because it is a very technical or specialist based subject.

Australia has land Courts, but currently in Fiji, our judges pretty much cover everything although some are civil judges, some are criminal judges but for cyber, would it not be better if we built judicial capacities, specialising their focus on that. Remember, when we talk about digital evidence and I will explain to you how the Police and the Government of Fiji has actually lost money. You can spend so much money on investigating something and when I say money I am talking about man hours of police time - serving production orders, going to the Telco's picking up information, investigating this, there and that, storing the information and then the data gets corrupted, and it is inadmissible. That is lost money - you cannot use it. You are looking at the financial and economic impact of not having a robust core locally, domestically.

Mr. Chairman, what I would put to the Committee is that we create a framework as a country. In terms of mutual cooperation - no problems if a country asks us and we are willing and we have the capacity to produce, we can produce. But to be legally bound to produce - that is the issue. Do we have the financial capacity? Do we have the capacity - do we have the manpower? I would say if they want to help us build a two year plan on how to strengthen the judicial systems, how to strengthen the Cybercrime Unit - to me personally they should be having their own 'building'.

The last time which was several years ago, there were five staff but for something like this, you need people and specialist training and not only that - judges need to be trained, parliamentarians need to be trained,

everyone basically needs training and even I need training. The drafters need training and we cannot let countries bully us or push us into doing something that we really do not have the capacity to do. They can give us free trips easy, fly to Europe enjoy a cocktail here and there, each year go and see the Eiffel Tower or the farms

in Geneva but the bottom-line is what is it costing the ordinary person in Fiji? Would that money have been better spent in health - strengthening the health care systems in the rural outskirts? That money could have been better spent in helping single mothers who are struggling to find a job with the Ministry of Labour, Ministry of Women.

That is why esteemed members of this Committee, I do not envy your job. In your hands you hold the fate of this nation that we dearly love so much. Your deliberations as team members of the Committee, will literally affect our nation. I have every faith that in this room you are not there by accident - each and every one of you are there by design and God put you there for such a time as this so that you can make decisions, and I know that God is giving you the wisdom to be able to lead our nation. I know that as you deliberate and go through the multiple content that people have given in, and as you comb through it, that you are going to have the wisdom to know what to do. I have every faith in you. Do you have any questions for me?

MR. CHAIRMAN.- Thank you, Salanieta, for those very inspiring and comprehensive report and the guidance that you also gave to this Committee. It is ironic that you made reference to the health systems as I am the Assistant Minister for Health, if you do not already know. Anyway, I open up the floor for any questions from the Members.

HON. S. ADIMAITOGA.- Mr. Chairman, through you, first of all I would like to thank you for such a comprehensive submission this morning. It has opened our eyes. I was looking at an angle as you have mentioned, the old dress and now we are trying to come up with mending, maybe it is torn, but then what I am looking at is, why do we not get new material and sew the same pattern as that one but in a very modern way. Do you have any effective way to help societies in meeting the challenges of cybercrime? Each project and organisation may have its own formula to make this work. Does Pacifica Nexus have any formula to make this work?

MS. S. TAMANIKAIWAIMARO.- Shall I take all the questions and then provide the answer – are there any more question?

HON. DR. S.R. GOVIND.- When Mr. Chairman asked you to introduce yourself, you did not really introduce yourself, because now with such depth of knowledge, I would like to know what is your background. What are you doing there, or what you have been doing in Fiji?

MS. S. TAMANIKAIWAIMARO.- You are very kind, Sir. In terms of professional training?

HON. DR. S.R. GOVIND.- Yes, everything and your work.

MS. S. TAMANIKAIWAIMARO.- I am a lawyer by profession and I have worn several hats. I have worked in private practice. I have also worked as a Regulator for the securities market, at that time it used to be CMDA, but that has been absorbed into RBF. I have also worked in the Pacific Islands Forum Secretariat to manage the Treaty depositories, when countries signed or ratified them so I used to look after Treaties and assist the legal advisor at that time.

I started a think tank in 2011 called Pasifika Nexus and that has been my pet project. I am the founder and director of Pasifika Nexus where I do fun things like this, make submissions or help people - it is more like a think tank. I also used to manage the Japan Pacific ICT Centre in the University of the South Pacific and I used to be Group Regulatory Counsel for Telco which was actually Telecom Fiji. I am based in England now.

In terms of my involvement in cybercrime and cyber security - at the time they had Cabinet and there was no sitting of Parliament and I was part of Teleco. Cabinet appointed me to chair the Cyber Security Working Group which was multi-stakeholder and included the cybercrime units - the Fiji Police Force and the Ministry of Defence. We reported to the Chief Protocol Officer at the Ministry of Defence and our first workshop was held in Nadi with basically representatives from all the industries. Before that workshop, I wrote a paper in 2011 and passed it on to Parliament, and made recommendations as well. That has pretty much been my background but I practice diversely, yes.

HON. DR. S.R. GOVIND.- Very good.

MR. CHAIRMAN.- Thank you, Ma'am.

MS. S. TAMANIKAIWAIMARO.- I am just an ordinary person from Tailevu.

MR. CHAIRMAN.- So just your response to the questions from honourable Adimaitoga. Thanks, Sala.

MS. S. TAMANIKAIWAIMARO.- Yes. The honourable Member asked about an effective way to tackle head-on cybercrime in Fiji? I would say we need to strengthen the core. As you can see in the current Act, I find it very deficient - it is just computer-related offences, very poorly drafted because it is mirrored on old law.

I took you through the historical context of the Budapest Convention and personally I feel that was back to front. I just want the people of Fiji to know that just because something comes from the West, comes from Europe, it does not make it better. It does not mean that it is posher. Personally, *tavioka* is posher than bread and *lumi* is posher than caviar. So we have to remove that mindset and we have to see what we have, build what we have, which is build our laws.

I would recommend that the Solicitor-General's Office do a robust analysis of the domestic laws - look at what the lacunas are, no shortcuts. Look at what the lacunas are and how we can strengthen it. Have we addressed the different categories? And look at capacity; prosecutors – are they trained, police – are they trained? How are we storing evidence?

I have also been a defence attorney, and it is very easy to throw out evidence and make evidence inadmissible, which means hundreds and thousands of man hours, dollars' worth of police hours being thrown out just because that thing is not stored, or properly kept because we just do not have the capacity. And we cannot blame the Fiji Police Force because they are doing amazing work, with the budget that they have. I will say that there are some aspects about the Cybercrimes Act that are excellent but largely, I would say build the core, build Fiji in a holistic approach. Did I answer that?

HON. MEMBER.- Yes.

MR. CHAIRMAN.- Time has caught up with us but we sincerely thank you for your submission, your contribution to the Committee this morning or evening in your time and wish you a blessed evening. If there is any departing comments, the floor is yours, Madam.

MS. S.T. TAMAINIKAIWAIMARO.- Thank you Mr. Chairman, Sir, I saw that one of your esteemed Members raised his hand. Did he have a last question, so I can address it in my parting thoughts?

HON. DR. S. GOVIND.- This is very important, Sala. Listening to you, we have been told that the United Nations (UN) is under the process of doing a similar Convention which will be presented to the UN General Assembly next year, so my direct question to you is that, should Fiji wait and look at that UN Convention before ratifying this one?

MS. S.T. TAMAIKAIWAIMARO.- Absolutely! Besides, we have already met the obligations of the Budapest Convention. In creating a document that 90 percent we have domesticated whatever is in the treaty, we have literally collaborated and affirmed. The bit that is tricky though is that, the minute we sign up, the mutual co-operation is what it means financially for us. It is different if they had a budget for it. That is a very good question and I will use it to wrap up as a parting-shot to say again that context shapes meaning.

Mr. Chairman, and honourable Members of the Standing Committee on Foreign Affairs and Defence it has been my absolute privilege to address you. It has been an honour, thank you so much.

The Committee adjourned at 10.22 a.m.

The Committee resumed at 10.30 a.m.

Interviewee/Submittee: Datec Fiji Limited

In attendance

Mr. Pramendra Pal - Pre-Sales and Sales Bid Manager

---

MR CHAIRMAN.- Ladies and gentlemen, before us this morning we have the Sales Manager from DATEC, Fiji. Please, introduce yourself and take us through your submission, after which we will raise questions. The floor is yours, Sir.

MR. P. PAL.- Mr. Chairman, and honourable Committee members, on behalf of Datec Fiji Limited, I would like to extend our appreciation for giving us an opportunity to make a submission towards the Convention on Cybercrime. I am Pramendra Pal and I head the Pre-Sales and Sales Bid team for Datec Fiji Limited. This team is primarily in place to respond to all the tenders, and respond to all the queries that come in from the customers, and a majority of that has been coming in, in terms of security. There is an increase in the number of security tenders that have been coming out, regardless whether it is for government, utilities or even corporates. Our submission is based on what we have seen.

The world is witnessing an exponential increase in cybercrimes. One of the latest examples being “OPTUS massive data breach” in the month of September that had exposed about 40 per cent of the populations’ personal data. Based on that, proactive measures are necessary to control or reduce each breach by implementing required governance frameworks and processes aligned with criminal justice, judiciary, prosecution and law enforcement.

To prevent cybercrime, companies, authorities and even individuals need to implement cyber hygiene to keep sensitive data secure and protect it from theft or attacks. It is necessary to defend against sophisticated threats and collaborate to build more secure and resilient infrastructure in the country. To maintain an evolving and proactive secured posture, all the stakeholders should implement sound practices, framework and solution to prevent cyber breaches.

Mr. Chairman, not only cyber security practices but also CERT is necessary in the country. Hence, as an ICT solutions provider in Fiji and the South Pacific, we recommend a national legislation to deter and combat cybercrimes. However, as becoming a member of the Convention concerns national and international co-operation, exchange, compliance and concerns nations security, a decision on joining the Convention should be made subject to approval from the Ministry of Foreign Affairs, Information and Communications, Defence, Financial Intelligence Unit and Human Rights.

MR. CHAIRMAN.- Thank you, Mr. Pal for the brief overview on the Convention from your organisation. Honourable Members, do you have any questions for Mr. Pal at this point in time?

HON. L.S. QEREQERETABUA.- Mr. Chairman, through you, Mr. Pal, you mentioned CERT. Can you just explain that to a lay person please?

MR. P. PAL.- Mr. Chairman, CERT is a response team put in place and referred to as Computer Emergency Readiness Team (CERT). It can even be known as Computer Emergency Response Team. This is a 24/7 system that monitors everything.

HON. P.W. VOSANIBOLA.- Mr. Chairman, through you, Mr. Pal just a question. In the last paragraph of your submission although we have the Cybercrimes Act 2021 but still you mentioned that you recommend a national legislation to deter and combat cybercrimes. What is your view on the current Act – does it not fully take into account what you have mentioned?

MR. P. PAL.- Mr. Chairman, this is something not to deter from the Act, it is just something that we can add on in place to get more security terms that can be available to individuals and companies. Adding to that, we have gone through a discussion point whereby cyber hygiene needs to be implemented for corporates, businesses and even individuals as well. Some of those hygiene are if you can implement a set of recommended securities in place.

Currently, if there is a company to be enrolled, there is nothing in terms of cybersecurity that goes as a kick-off in terms of if we are applying for a business license or anything. Security is not available at the moment to do that. Just to combat all those, we can always put in place things like point protection, multifactor authentication, secured password management. The major issue or concern within the companies currently are the secure password management. Most of the companies do not even use password walls - people are sharing passwords and for example, if there is a company and individuals were sharing passwords and they come up with passwords, the actual password they would put is Password 1. Anyone can go in, hack the system and get as much data as possible. So just putting those in place aligning it to the Act would be more beneficiary.

MR. CHAIRMAN.- What you are suggesting maybe a policy matter to run parallel to the Treaty?

MR. P. PAL.- Yes.

HON. S.R. GOVIND.- You mentioned building a more resilient infrastructure so from your point of view, what specific infrastructure should the Government be looking at and what sort of resources are you talking about?

MR. P. PAL.- Mr. Chairman, just to recap on what we had discussed earlier. This is something in terms of putting health and security in place and this will eventually improve our infrastructure. As mentioned, if we put cyber security practices in place, the infrastructure itself would be made much better for people to use. Because in the existing infrastructure, whatever they currently have, is just to implement some measures, policies and procedures that will be in place to control it.

HON. DR. S.R. GOVIND.- What are these infrastructure? What are the components of the infrastructure?

MR. P. PAL.- The components of the infrastructure are examples of Next Generation Endpoint Protection. Commonly, people only think that if they install an antivirus, they are protected, but it does not work that way anymore. Now you need to have Firewalls in place with all securities, so when people try and breach your policies, they can be blocked out, for example, one is just the end point protection and the other one is the multi-factor authentication.

If you have the multi-factor authentication, if someone needs to access any of your files, there would be a notification into your handheld devices or an authenticator app that would ask you to allow that person to actually have access to that. So putting this in place, would help. Even most of the companies currently do not have business continuity and disaster recovery. Disaster recovery - currently people would just do a normal backup and put it off site. But, what would happen if there is an unforeseen circumstance? You cannot get the data that has already been there, readily available to anyone within a spin of minutes. In terms of that, you need to put in things like business continuity and disaster recovery.

HON. L.S. QEREQERETABUA.- Mr. Chairman, just to follow on from that reply to honourable Govind, Mr. Pal, is that a weakness of the individual businesses not seeing business continuation or emergencies as being an important part of the business? The angle I am coming at is, it is not so much something that has to be legislated with bringing in the Budapest Convention, but more, just telling businesses how important cyber hygiene is for them.

MR. P. PAL.- Mr. Chairman, yes, just following through what you have mentioned. It is something of a business practice that needs to be in place. It is not something that needs to be driven through the Convention, but something businesses need to have in place.

HON. P.W. VOSANIBULA.- Mr. Chairman, can you just elaborate on that breach, the OPTUS massive data breach and which part of our population were really affected - that 40 percent?

MR. P. PAL.- Mr. Chairman, this data breach was for OPTUS and it is a telecommunication industry. The data breach was through their security level and in terms of that 40 percent of the population were affected, because most of the customers in Australia use OPTUS. Along those lines, 40 percent of the population's personal data, which is their names, emails, date of birth and all the details were leaked out, so this was in line with identity theft as well.

HON. P.W. VOSANIBULA.- This is in Australia?

MR. CHAIRMAN.- Honourable Members, if there are no further questions, Mr. Pal, I take this opportunity on behalf of the Committee to thank you for availing yourself, and if there are any other pressing questions and queries that the Committee may have, that you will avail yourself at a later date and time. If you have any departing comments, the floor is yours.

MR. P. PAL.- Mr. Chairman, once again thank you for allowing Datec for this opportunity to make a submission. We are more than happy to assist you with any clarifications that may come in, and we can work along with the secretariat to make a submission.

The Committee adjourned at 10.45 a.m.

The Committee resumed at 10.50 a.m.

**Interviewee/Submittee:** Fiji Police Force

In attendance

1. Mr. Aporosa Lutunauga, Assistant Commissioner of Police/Chief Admin Officer
  2. Mr J. Fong, Chief Planning and Research/Dog Training Officer
  3. Mr Avinesh Chand, Assistant Superintendant of Police/Officer-in-Charge, Cybercrime
  4. Mr H. Singh, Senior Police Officer, Planning Office
  5. Ms Paulina Rasila, Senior Police Officer, Planning Office
- 

MR. CHAIRMAN.- Ladies and gentlemen, before us we have the Fiji Police Force, ably led by the Assistant Commissioner. Sir, could you introduce your team, after which you can make your submission followed by a question and answer session.

MR A. LUTUNAUGA.- Thank you Mr. Chairman and members of this respectful Committee, first of all on behalf of the Commissioner of Police, I wish to convey his apologies for not attending as he is tied up with some official commitment this morning.

(Introduction of team members)

Mr. Chairman, members of the Committee, ladies and gentlemen, my task this morning is to present the Fiji Police Force contribution towards the Committee's review of the Cybercrime Convention, otherwise known as the Budapest Convention. First and foremost, the Fiji Police Force fully supports the Fijian Government in the process of reviewing the Cybercrime Convention. This is critical to our relations with other countries in terms of development, aid, foreign direct investment and multi-lateral partnerships.

The scope of aspiring to have full rights to access the implementation of the Convention, shall be fully realised should Fiji accede to the Convention. This will also bolster Fiji's commitment towards cybercrime in Fiji and the Region in terms of the effective execution of duty, as law enforcement officers. In addition, the Convention is a vital tool for the protection of all Fijians as the legal framework surrounding cybercrime shall be strengthened and the rights of all citizens shall be upheld.

As a law enforcement agency, the Fiji Police Force is sanctioned under the Government's National Development Plan to protect all Fijians from environmental risks and natural disasters, transnational crimes in the form of human and drug trafficking, food and nutrition security and public health risks and financial and cybercrime.

The Fiji Police Force therefore strives to enforce laws and legislations that falls under its mandate, and that is the Cybercrimes Act 2021. At the outset, the Cybercrimes Act 2021 comprehensively addresses

cybercrime by prescribing computer-related and content-related offences, providing procedural requirements including the collection of electronic evidence and international cooperation, providing the remedies in relation to cybercrime and for related matters. Therefore, Mr. Chairman, Sir, the ratification of the Convention will synchronise the Cybercrimes Act 2021 that was recently passed in Parliament on 11 February, 2021 as it mirrors the various sections of the Convention.

Fiji also has the Online Safety Act 2018 for the promotion of online safety, deterrence of harmful electronic communication and for related matters. The growing threat of the global cybercrime to Fiji and the Pacific is a concern. There is an urgent need for the Fiji Police Force to have full digital access to and be compliant with other law enforcement jurisdictions for international cooperation on the investigation, enforcement and prosecution of cybercrime. In terms of data security, Mr. Chairman, Sir, the Fiji Police Force has a secure IT system that has been safeguarding our digital information from corruption, theft or unauthorized access.

The recognition to be fully equipped with investigative enablers such as the Budapest Convention is most needed now than ever. There have been difficulties faced whilst trying to locate the suspect if a case is reported through social media and it is even worse when a suspect is based in another country. Strengthening such mechanisms is therefore necessary to ensure that perpetrators are registered, located and dealt with.

Further to this, a cybercrime is registered as Police Enquiry Paper (PEP), this is an investigation paper as soon as the report is received either at the station level or for referral at the CID HQ and is only converted to a registered case when a perpetrator is arrested and charged. There have also been some PEP cases pending since 2015. Some PEP cases have been filed as complainants do not want any police action.

In terms of cybercrime statistics, Mr. Chairman, Sir, a total of 45 cases were registered between the years 2016 to 2021. This includes the following cyber related offences:

- Authorised modification of data held in a computer;
- Serious computer offences;
- Unauthorised modification of data to cause impairment;
- Unauthorised modification of restricted data;
- Causing harm by posting electronic communication, and
- Posting an intimate visual recording

In addition Mr. Chairman, Sir, the Fiji Police Force registered a total of three females and eight male victims, and one female and six male offenders from 2016 to 2021. The statistics may not be that significant since Fijian people are not so forthcoming in reporting cyber related cases. This may be due to increased access to technology whereby criminals need not be physically present at that scene to commit a crime. Also, cases have not been reported due to the social stigma faced by victims who reported such cases. The Fiji Police Force therefore shall continue to provide data on cybercrime to the Fiji Police Force

relevant stakeholders, strive for a more inclusive approach to enhance our reporting structure and provide gender disaggregated data on cybercrime for the benefit of our relevant working partners as we effectively deal and respond to cyber related cases.

Mr. Chairman, Sir, the Fiji Police Force continues to venture into engaging with external stakeholders through its international relations portfolio to explore avenues in advancing Fiji's response against cybercrime. Hence, the continued commitment on capacity building to effectively response to cybercrime. Police Officers have been attending training locally and internationally in collaboration with our partners such as the Australian Federal Police and Cyber Safety Pacifica. This will ensure that the Fiji Police Force is well versed with cybercrime and the laws surrounding it. Knowledge on technology and its evolving apparatuses needs to be enhanced since the criminal environment is changing and computer hackers and genius operates in the border-less realm of cyberspace.

Currently, Mr. Chairman, Sir, no proper technological equipment is available such as phone extraction machines that can retrieve messages and calls. However, the Fiji Police Force is working on securing a phone extraction machine to address cybercrime issues. The Fiji Police Force has to continue to forge ahead to be on par with the global digital system. Several parties are joining hands in realizing the national intent of building a safer Fiji. The Fiji Police Force have been capitalising on inter-agency machinery to reinforce the existing legal framework under the whole of government and whole of population approach in creating awareness on cybercrime to schools, villages and communities. However, more concerted efforts shall be manifested on awareness should Fiji ratify the Cybercrime Convention.

Furthermore, Mr. Chairman, the Fiji Police Force is appreciative of the collaborative efforts by regional and international counterparts in solving some challenging cases of cybercrime that has emanated with the drug bust in Fiji. This Convention therefore shall allow the Fiji Police Force to contact and allow easy access to any member State that is a party to this Convention through their focal points for data information and evidence. The Convention shall also safeguard Fijian citizens from unnecessary exorbitant mandatory loss, bankruptcy and economic leakage, online defamation of character, suicide or any action that may be detrimental to Fijians.

On the ratification, Mr. Chairman and honourable Members, the Fiji Police Force fully support the ratification of the Cybercrime Convention as this will endorse Fiji's obligation towards its commitment, towards the international community and a global safety and security emanating from the ever increasing interconnectivity to the worldwide labyrinth of communication, information and telecommunication through various traditional and emerging means

Mr. Chairman and Members of the Committee that is the submission of the Fiji Police Force.

MR. CHAIRMAN.- Thank you, ACP Lutunauga for your very insightful report of your operations within the Fiji Police Force. Honourable Members, any question for Mr. Lutunauga and the team.

HON. P.W. VOSANIBOLA.- First I would like to thank Mr. Lutunauga for the very valuable information prior this morning. As you mentioned, the Fiji Police Force fully supports the ratification of this Convention, do you have the capacity and the infrastructure to deal with this cybercrime?

MR. LUTUNAUGA.- The Fiji Police Force, as I have stated is building its capacity in cybercrime as we speak. We are collaborating with our counterparts from overseas through our international relations focal point in building our capacity in cybercrime as we have our officer-incharge of cybercrime. Sometimes next week we will be opening up our new Forensic Cybercrime Office which will assist us in the implementation of the operationalising the Cybercrimes Act of Fiji.

MR. CHAIRMANMAN.- Just on that same question and your feedback, Mr. Lutunauga, what sort of operational hours is your team working in and what sort of human resource capacity do you have.

MR. LUTUNAUGA.- We are working 24/7 and we have got a team of 11 members currently which includes Investigating Officers and our IT Officers.

HON. L.S. QEREQERETABUA.- Through you, Mr. Chairman, I just wanted to ask you, Sir, or may be ask all of you, do you feel there are over laps between your KPIs and the KPIs of FICAC, in terms of investigating certain search and seizure of electronic gadgets and laptops, and so forth. Is there any overlap?

MR. LUTUNAUGA.- I think while they do not realistically overlap, FICAC runs only on abuse of office or corruption cases while we focus on the other criminal aspects of the criminal case under the Cybercrimes Act. There is a very fine line that separates these two. While they deal with financials as you have stated, we also deal with that but more on the criminal aspect, but different offences.

HON. S. ADIMAITOGA.- Through you, Mr. Chairman, since you supported the Cybercrime Convention, can you explain further on what have stated, because the Convention aims principally on harmonising the domestic criminal substantive law elements of offences and connected provision in the area of cybercrime? Can you explain further whether you are into that because you supported the Convention?

MR. A. CHAND.- Thank you, Ma'am, we are supporting that because most of our cases deal with criminals who are abroad. Once we get into the Budapest Convention it will be easy access with other countries. It is something like Interpol. We will get in connection with other countries in identifying the offenders, if possible we can always lay charges if there is some kind of understanding between the countries. Thank you.

MR. J. FONG.- Mr. Chairman, in addition to that response, for the information of the Committee most of our Police Officers have done studies abroad and we have connection with our colleagues from other countries so instead of going through the government to government approach, we have those

connections. So, if there is a case in a particular country, you need a particular suspect it is easy to go person to person, through your friends before we go with the government to government approach. Thank you.

MR. CHAIRMAN.- In other words you are running parallel to Interpol?

MR. J. FONG.- Yes, Sir.

MR. CHAIRMAN.- Honourable Members, if there are no further questions, on behalf of the Committee we wish to sincerely thank you Sir and the team for availing yourselves. If there are any sterling questions or queries during our deliberations that you will avail yourself should you be called upon. With those few words, Sir, if you have any departing comments, the floor is yours. Thank you.

MR. A. LUTUNAUGA.- Thank you very much, Sir. It has really been a blessing and privilege to be here today, again, to meet the honourable Members, and we wish this Committee all the best in your findings, Sir.

The Committee adjourned at 11.07 a.m.

The Committee resumed at 11.20 a.m.

**Interviewee/Submittee :** Fiji Human Rights and Anti-Discrimination Commission

In Attendance

Mr. Ashwin Raj

---

MR. CHAIRMAN.- Ladies and gentlemen, before us this morning we have the Director of the Fiji Human Rights and Anti-Discrimination Commission. Sir, the floor is yours after which we will have questions and answers.

MR. A. RAJ.- Good morning, Mr. Chairman and the honourable Members of the Committee, my gratitude on behalf of the Human Rights and Anti-Discrimination Commission for graciously extending an invitation to the Commission to be able to contribute to this important deliberation.

Consistent with these recommendations to the Parliamentary Standing Committee on Justice, Law and Human Rights on 30<sup>th</sup> June, 2020 in relation to the then Cybercrimes Bill, which has been enacted, the Commission supports the States commitment towards ratifying the Convention on Cybercrime otherwise known as the Budapest Convention, because Fiji already has a comprehensive legislative framework in place that encapsulates the most salient features of the Budapest Convention, and aligns the requirements of the Convention.

In countenance with the Convention, the Cybercrime Act introduces offences against the breach of confidentiality, integrity and availability of computer data and computer systems. These include the unauthorised access to computer systems, unauthorised interception of computer data or computer systems, unauthorised access in relation to computer data and computer systems, and unlawful supply or possession of computer systems or other device or computer data. It also introduces other computer and content related offences, such as, computer related forgery, extortion, fraud, child pornography, identity theft, theft of the telecommunication services, disclosure during an interview and investigation and the failure to provide assistance. The Act also introduces procedural measures and remedies in relation to cybercrime related offences and the protocols governing the collection of the electronic evidence and international cooperation.

The Convention on Cybercrime entered into force in 2004. It is the sole legally binding international multilateral Treaty that addresses the internet and computer related crime such as, infringements of copyrights, computer related fraud, child pornography and violations of network security. The Convention has created conditions and the possibility, not only for the criminalisation of certain cybercrime conduct and establish the procedures for the investigations of such transgressions, but also facilitates

investigations through coordination between nation States as well as build the capacity of Pacific Small Island Developing States, such as Fiji, through the provision of technical assistance, which will be critical in ensuring that the Convention is effectively implemented. It provides the most comprehensive framework for the development of national legislation and safeguards against cybercrime including increased cooperation between private entities, with criminal justice authorities of contracting State Parties.

As enunciated in this preamble, the objective of the Convention is to prioritise, and I quote: “A common criminal policy aimed at the protection of society against cybercrime, inter alia by adopting appropriate legislation and fostering the international cooperation.” Of course, the Commission has received complaints and some of the complaints in relation to cybercrime include non-consensual distribution of intimate images – these are complaints about intimate images and videos on social media platform via emails, which includes images of children, adolescence and adults, particularly in the context of relationships that would have broken down and now strained, and ensuing cyber bullying. The other very common complaint that we receive are complaints of hacking. The Commission continues to receive complaints relating to compromising digital devices through unauthorized access to an account or computer system to access intimate images and pictures particularly by ex-partners and again in strain relationships, identify theft is another complaint which constitutes acquisition of someone’s identity information such as name, residential address, family photographs and family history in order to impersonate someone on the social media platform such as *Facebook* and *TikTok*. We have received complaint in relation to online scams on platforms such as *Instagram*. A complainant was tricked into giving money by fake account holders on *Instagram*, by someone who was a crypto investor and crypto currency, of course, investing can take many forms ranging from buying crypto currency directly to investing in crypto funds and companies. You can also buy crypto currency using a crypto exchange or through certain broker deals.

Without taking much of the Committee’s time, we did make a very comprehensive submission in 2020 where we aligned the various provisions of the Cybercrime Bill and now Act of Parliament against that of the Convention. So I am more than happy to share that with the Committee and also the substantive submission in relation to the Cybercrime Bill as well because this is very consistent in terms of what we as a Commission have been saying thus far. So we have seamlessly mapped all of the clauses against all the Articles of the Convention to examine how the alignment happens and what are the imperatives behind of the clauses and each of the Articles of the Convention.

Very quickly the recommendations we are making are:

- 1) The Fiji ratifies the Convention on Cybercrime or the Budapest Convention to ensure compliance with the normative instruments.
- 2) That the moral and legal imperatives of the Cybercrime Convention and the Cybercrime Act be balanced with the State’s human rights obligations under its domestic procedures and international human rights law. I will be very happy to expound on this, should there be questions.

- 3) Prioritise awareness and advocacy on the legal and human rights ramifications of the Convention, the obligations on the State and the role of law enforcement agencies and private entities.
- 4) Strengthen the capacity of law enforcement agencies in the private sector in addressing the issue of intermediary liability.

With that, Mr. Chairman, thank you very much and I would welcome any questions you or Members of the Committee might have.

MR. CHAIRMAN.- Thank you Mr. Raj for your contribution this morning. You have highlighted some recommendations which we will definitely look at in our deliberation on the Convention.

HON. L.S. QEREQERETABUA.- Thank you Mr. Chairman, through you, I just wanted to ask Mr. Raj, thank you for your presentation, are any of the recommendations that you will be giving to the Committee around media protection, the protection of people in politics, in particular. As you know, we are going through, having elections soon, and this is one thing that has stood out in a few of the presentations that we have had from our submittees about media protection, protection of politically exposed persons. Will that be included in your recommendation?

MR. A. RAJ.- When I say that we need to carefully balance the moral and legal imperatives of the Convention and the Act and balance it with the State's human rights obligations under its domestic procedures international law. Obviously, I am not trying to preferentially frame which rights matter more than other rights because all of the human rights are indivisible and interdependent. So, one of the things that, of course, we need to keep in mind all the time is that the State has a positive obligation to ensure that citizens are able to receive, seek and impart impart information, but at the same time, I think we also need to be cognizant of the justifiable limitations that have been placed in law that are again very consistent in our Constitution as well as international covenants such as the Covenant on Civil and Political Rights. So, in particular if you look at the provisions around the right to free expression, including the right to press freedom; these are rights that are enshrined in our Constitution and at the same time, they are also recognized in the International Law as well which the State is a signatory to and has an obligation to uphold at all times. What we need to do is to strike a careful balance between these fundamental rights and freedoms that we must jealously guard at all times, because that is what enables a thriving deliberative democracy, at all times, not because we are on the cusp of an election but at all times people should be able to express ideas and engage with institutions no matter how divergent those perspectives might be.

You and I can fundamentally disagree over a politically contentious issue but we should be able to raise those things, but at the same time (I think) as a democracy we also need to understand that these rights and freedoms are not unfettered - they come with a responsibility. Therefore the fundamental point is that we must at all times ensure that we recognize the justifiable limitations that come and the responsibilities that come with those rights and freedoms, to ensure that the exercise of ones rights and freedoms does not interdict the rights and freedoms of someone else.

The limitations are very clear in both our Constitution and the International Law, that this right and freedom does not allow you to incite the advocacy of hatred on any of the prohibited grounds of discrimination - it might be around race, religion, ethnicity, sexual orientation, gender, age, disability. Our Bill of Rights in terms of the prohibited grounds is quite expansive. It is also about making sure that there is no incitement of communal antagonism, of propagation of war but at the same time I think the Convention and the Act in place also creates a very fertile ground for developing jurisprudence in this field. I think it is good that we have got a robust Bill of Rights, we have ratified the core Treaties and Convention, the ICCPR in particular and now we have the Budapest Convention. This is why I am very glad that the State has taken this trajectory because once we ratify Conventions we are always on the path of human rights.

There are obligations incumbent on the State which means that it is not operating in abeyance, it is not in a state of inertia, the job really becomes one of seamlessly mapping where our ancillary legislations are against all of our international human rights obligation. For that reason I think this is very very important and we need to continuously sort of bring the international instruments to bear on our domestic procedures. That is why I keep saying it is the delicate dance between what our domestic procedures are saying and what our obligations are, under the international human rights law - and ensuring that people are able to enjoy the fundamental rights and freedoms including the freedom of the press but taking full cognizance of the justifiable limitations that have been put in law for very good reason. Thank you for the question.

MR. CHAIRMAN.- Thank you Mr. Raj. With your complaints, where to from there? Who is the other stakeholder or just do you deal directly with them? You are getting all the complaints on a daily basis.

MR. A. RAJ.- Thank you very much for the question Mr. Chairman, Sir and honourable members of the Committee, when the Commission receives complaints of this nature, of course we liaise very quickly following an assessment of whether it is a complaint that falls within the purview of the National Human Rights Institution or does it exceed our jurisdiction and needs to go to another relevant authority. In quite a few instances we refer matters to the Cybercrimes Unit of the Fiji Police Force and we also refer matters to the Online Safety Commission as well. This of course underscores the need for us to not look at the various pieces of legislation and cyber laws. We need to make sure that there is synergy between the Act that governs the National Human Rights institutions, the Cybercrimes Act in place, Criminal Procedure Act and the Crimes Act.

Look at what the roles of parallel statutory bodies and independent institutions are. One of the things we do as a Commission we are not in a habit of delegating and disappearing. If we have referred a matter to an institution whether it be the Fiji Police Force or the Online Safety Commission, we always get back to those institutions to see what is happening to these complaints because we also need to see whether people are able to get the kind of remedy that they expect from these institutions, and whether the legislation is adequately protecting them or it is just a putative claim and law. That kind of triangulation is extremely important and this is why the Convention and the Act can be very robust and salutary.

It is incumbent on institutions that have the fundamental role of monitoring compliance to actually do that, because the legislation on its own cannot unfortunately protect the kind of adequate safeguards that we actually need. I think the purveyors of law have done a good job of making sure that we have these legislative frameworks in place. It is incumbent on institutions like ours to work collaboratively with each other and make sure that these instruments have teeth and they deliver to the people, and that people feel comfortable if they go to an institution that they will get the kind of remedy they are looking for - if they cannot then where can they actually go. And that also brings to bare this other point, Mr. Chair, about education and awareness.

It is so important that the citizens of this country are fully empowered with that knowledge about what the laws are saying. We need to translate into the vernacular. We at the National Human Rights Commission do that - we translate things in *Hindi*, and *iTaukei*. We look at the rights of arresting and detaining persons and we even translate it in *Chinese*, *Rotumans*, *Bhanaban* and all of that. For people who have access to the lexicon they understand the law, they know the nuances, people like us in this room - it is almost like preaching to the choir.

What is important is that ordinary members of the public understand what the legislation is saying. What is important is that Police Officers at the level of Police Stations understand what the law is saying, what the remedies are and what they should be doing, before people carefully assess and say, I am sorry this is a complaint where we cannot do anything because it is in online. It was a fake identity and I am sorry we cannot do anything or, we do not have that technological knowhow in terms of how to deal with encryptions, to access this account which has been deactivated and all of that.

I really think that we need to place this Convention and the Act in the context of these largest societies in which we are operating. There has got to be much more robust conversations between all of the stakeholders. We need to work collaboratively and constructively with each other because the goal is collective. But also, we cannot do it without having the kind of engagement and conversations with society at large and that means all stratum of societies including those in rural, remote, maritime areas, and even persons with disabilities are also victims to cybercrime and a lot of times they are not able to access institutions of remedy. This is where I think the role of a National Human Rights Institutions is an extremely important one - to translate these legislations into everyday language so that people can understand that they own the legislation. They are not alienated from it and then be able to constructively engage with the body of law to get remedy, develop jurisprudence, have robust conversations and engage with institutions like yours, to make sure that we raise levels of discourse and discussions so that we are able to do justice to this ratification and the strong and salutary legislation framework we have in place.

MR. CHAIRMAN.- Thank you, Mr. Raj. It is very encouraging to know that your Commission is translating into the vernaculars - it is very important I should say. Honourable Members, if there are no further questions, I take this opportunity to sincerely thank Mr Raj once again for availing himself. If there are any other pertinent questions that the team may have that you will avail yourself at a later date.

MR. A. RAJ.- Thank you very much, Mr. Chairman and Members of the Committee. Thank you for all that you do. I will make sure that you receive an electronic copy of this submission but also you know the submission we made in 2020 about the Cybercrimes Act itself so that you have both and you can place the Commission in the context in which I was speaking.

MR. CHAIRMAN.- *Vinaka.*

The Committee adjourned at 1.41 p.m.

**[VERBATIM REPORT]**

**STANDING COMMITTEE ON**  
**FOREIGN AFFAIRS & DEFENCE**

**TREATY/CONVENTION**

**Budapest Convention on Cybercrime**

**INSTITUTIONS:** (1) Office of the Director of Public Prosecutions  
(2) Fiji Women's Crisis Centre

**VENUE:** Small Committee Room (West Wing)

**DATE:** Tuesday, 11<sup>th</sup> October, 2022

**VERBATIM REPORT OF THE MEETING OF THE STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE HELD AT THE SMALL COMMITTEE ROOM (WEST WING), PARLIAMENT PRECINCTS, GOVERNMENT BUILDINGS, ON TUESDAY, 11<sup>TH</sup> OCTOBER, 2022 AT 10.25 A.M.**

**Interviewee/Submittee:**

**Office of the Director of Public Prosecutions**

**In Attendance:**

1. Mr. Christopher Pryde - DPP
2. Ms. Jayneeta Prasad - Principal Legal Officer
3. Ms. Farisha Ahmed - Media Liaison Officer

---

MR. CHAIRMAN.- Honourable Members, members of the public, the Secretariat, ladies and gentlemen, a very good morning to you all and it is a pleasure to welcome everyone, especially the viewers who are watching this proceeding.

For your information, pursuant to Standing Order 111 of the Standing Orders of Parliament, all Committee meetings are to be open to the public, therefore, please note that this submission is open to the public and media and is also being streamed live on Parliament's website, social media online platforms and the Parliament Channel on the Walesi Platform. For any sensitive information concerning the matter before us this morning, that cannot be disclosed in public, this can be provided to the Committee either in private or in writing.

Please be advised that pursuant to Standing Order 111(2), there are only a few specific circumstances that allow for non-disclosure and these include:

- National Security matters;
- Third party confidential information;
- Personnel or human resources matters; and
- Committee deliberation and development of Committee's recommendation and reports.

This is a parliamentary meeting and all information gathered is covered under the Parliamentary Powers and Privileges Act. Please bear in mind that we do not condone slander or libel of any sort and any information brought before this Committee should be based on facts. In terms of the protocol of this Committee meeting, please minimise the usage of mobile phones and all mobile phones to be on silent mode while the meeting is in progress. Allow me now introduce the Honourable Committee Members.

(Introduction of Honourable Members, Secretariat and Hansard)

Today, the Committee will be hearing a submission on the Convention on Cybercrime otherwise known as the Budapest Convention. For the purpose of the viewers who are joining us this morning, allow me to give a brief explanation on the Treaty. The Convention on Cybercrime, also known as the Budapest Convention,

provides a comprehensive and coherent framework on cybercrime offences and electronic evidence. It serves as a guideline for any State developing comprehensive national legislation against cybercrime and as a framework for international cooperation amongst States Parties.

To date, the Convention has 67 member States, which includes Australia and Tonga from the South Pacific Region. Pursuant to Article 37 of the Convention, any other State Party, such as Fiji, can become a Party by accession if the State is prepared to implement the provisions of the Convention and upon invitation to accede to the Convention after consultation and approval of Parties.

With the extreme effects of global cyber threats and attacks on critical sectors such as finance, ICT, energy, water, emergency services, public safety, health, public services, aviation and e-government infrastructure, becoming a Party to the Convention will enhance Fiji's ability to combat cybercrime, with international support and assistance particularly in relation to continued capacity building, to better equip Fiji's criminal justice authorities, including the judiciary, prosecution and law enforcement agencies.

Ladies and gentlemen, before us this morning, we have the Office of the Director of Public Prosecutions and we have Mr. Christopher Pryde, who is the Director. Without further ado, I would like to welcome you and request that you introduce your team and continue with your submission, after which we will have a question and answer session.

MR. C. PRYDE.- Mr. Chairman and honourable Members of the Committee - good morning. First, thank you for affording me the opportunity to present the submission of the Office of the Director of Public prosecutions this morning. I am grateful for the extension of time that was also granted so that we could prepare our submission, and I am also grateful for the opportunity to come and address you in person this morning.

Before I begin, I would like to introduce, Ms. Jayneeta Prasad, she is one of the prosecutors in the Office of the DPP. She is a Principal Legal Officer and heads the Serious Fraud Division and she also heads our Mutual Legal Assistance and Extradition Section in the Office of the DPP. I also have Ms. Farisha Ahmed who is our media liaison officer.

Sir, in essence, our Office supports Fiji's accession to the Convention but with reservations. We have confined our submissions to a letter which we sent out this morning. I do have spare copies of this letter you like. I know it is a little bit short notice, but we were still making some amendments to it, first thing this morning. Perhaps if I take you through the main parts of it, there is not very much and certainly, we are available to answer questions.

The first part of our submission really was just involving an analysis of the Convention and Fiji's existing legislation. The Convention is making it mandatory for State Parties to criminalise certain offences and we note that the Cybercrimes Act has been enacted but is not yet in force. The Cybercrimes Act is the main legislation designed to ensure that Fiji will conform to its obligations under the Convention. If Fiji accedes to the Convention, other Acts will also require amendment but I think the government is to be commended

for getting the legislation in place first before ratification. This does not often happen, so it is good that we have got some solid legislation in place before we consider accession to the Convention.

We have just a couple of comments in terms of what the Cybercrimes Act does or does not do in relation to what we would be obligated to do under the Convention. We had looked at the issue of deletion and alteration but we have concluded that the Cybercrime Act does sufficiently deal with that as an extra offence. There is, however, a need to deal with the Juveniles Act because the Convention is quite clear about the need to criminalise possession of child pornography under Article

9(1)(e) - that is not currently criminalised under Fiji's laws at the moment but I can say a little bit more about that in a moment.

The main thrust of our submission concerns international cooperation and in particular extradition and mutual legal assistance. In terms of extradition, the Convention does not place additional requirements on extradition and they are all adequately outlined in the Extradition Act that Fiji has which is the 2003 Act. We also preserve certain things - the allowance for us to choose to prosecute instead of extraditing. We have a dual criminality requirement for extradition requests made to Fiji but as I have mentioned, with the exception of possessing child pornography which is not an offence in Fiji, the offences outlined in the Convention would all be considered extradition offences.

Dealing with mutual legal assistance, the main Act that we have that governs that in Fiji is the Mutual Legal Assistance in Criminal Matters Act and this is being modified somewhat by the Convention. Perhaps if I could just take a moment to explain how the Mutual Legal Assistance in Criminal Matters Act operates at the moment, MACMA as we call it - we have used this for a number of application requests from foreign governments. The most recent one was to do with a U.S request to execute a seizure warrant issued by an American court against the Russian super-yacht *Amadea*.

This involved going from a request from the U.S authorities through Foreign Affairs, to the central authority in Fiji which is the Attorney-General who considers the request, balances foreign policy requirements and then sends an authority to proceed to whichever agency is tasked or is the necessary agency to deal with the matter. In this case it was my office, (the DPP's office) and the police and in actual fact there were a number of other agencies involved in that. There was immigration, there was FIRCA, there was the Maritime Authority, there was the port of Lautoka, as well as the police, the US Embassy, Attorney-General's Office, my office and the Courts. All of these requests go through the AG and the AG considers it and an Authority to Proceed goes to whoever, in this case it was the Police and the DPP's office. We carried out the request under the terms specified in the Authority to Proceed. We have dealt with quite a number of requests over the years and I can say that they are dealt with expeditiously and especially in this case, we were able to deal with the matter very quickly, without delay at all, and this was all completely in accordance with the Mutual Legal Assistance in Criminal Matters (MACMA).

Mr. Chairman, Sir, the MACMA allows for the expedited means request this is also what is required under the Convention. We do not have dual criminality requirements for mutual legal assistance that is also consistent with the Convention, we are not required to. With the exception of the Financial Intelligence Unit none of Fiji's law enforcement agencies do spontaneous sharing of information and the Convention also

makes that discretionary. The appointing of a Central Authority is all consistent, grounds for refusal, confidentiality is extremely important and that needs to be respected at all times, so for that it is fine.

We get to Article 29 and Article 30 and what we have here in the Convention is relating to preservation of stored computer data and preservation of that data before a formal request is sent, but where it differs is that under Section 13 of the MACMA the Attorney-General must authorise a law enforcement agency such as the Police, by way of an Authority to Proceed, to conduct the search and retrieve evidence which is by way of a Magistrates Court warrant. There is a conflict here between the Cybercrimes Act and MACMA and of course the Cybercrimes Act is consistent with the Convention but where we have the conflict, we see it as overriding the protections given under MACMA. In terms of the Cybercrime Act being consistent with the Convention, it is but we say it is inconsistent with MACMA, and I will say a little bit more about that in a moment.

But other things are similar for example a formal request being made. There is an issue though in relation to having a point of contact 24 hours, seven days a week. My office is intrinsically linked to criminal matters, mutual legal assistance and extradition and we do not have the ability to be able to man something 24/7 or to assist any contact points who may be nominated. I mentioned the *Amadea* case - that is an exception but that was an example of a 24/7 network because there were many different agencies including us, involved and because of course the time difference we were getting requests coming through from the United States through the Attorney-General's office to act sometimes very quickly (you know 1-2 o'clock in the morning) in order to preserve evidence and to ensure that the request was fully complied with. The 24-7 network is a good idea but it would require adequate resources to my office but also to other agencies that would do that. I know that the Legal Aid Commission, for example, has something similar but I am not quite sure how they manage their resources but 24 hours, 7 days a week would need to be adequately resourced, that is our strong submission on that.

In terms of the Cybercrimes Act, it is our view that it is important that the Attorney-General as the central authority under MACMA, be maintained as the first point of contact under the Convention and under the Cybercrimes Act, so as to act as a filter and protection against unsanctioned or fraudulent requests, and to allow the Fijian Government to balance its foreign policies with those of the requests from a requesting party. The ability of foreign requesting parties to circumvent Fiji's competent authority and go directly to a law enforcement agency such as the Police, potentially risks two things - it allows a request from a malevolent source such as a criminal organisation to obtain confidential information, because what Section 30 of the Cybercrimes Act says is that an enforcement agency in a foreign country can directly contact the enforcement agency in Fiji and have them retrieve that data and disclose that data, without going through the Attorney-General.

This can also happen even if it might be in conflict with Fiji's foreign policy position on things, for example, if the enforcement agency comes from a country which Fiji has limited diplomatic relations, we might not want to accede to that. Coming back to the *Amadea* case, this was something that was raised in court where the defence lawyers had said to us - "you are just a rubberstamp you know because this a request from the US and you are just filing it in the court". So what would happen if the Russians made a request - would you just do the same thing and I said, no we would not because their request would come through the Attorney-General's Office and he can balance that. Of course he looked at the request from the US and decided that

it was consistent with Fiji's stand and he acceded to the request. What would happen if it was from another country, another enforcement agency - a different consideration needs to be made but that is for the Attorney-General and for the Government to make, it is not for the individual enforcement agencies to make and that is the danger of that sort of thing.

We were also aware of this when we were having discussions with our colleagues in the Ukrainian Prosecution Office because before we were able to talk to them. They also went through quite a procedure to ensure the *bona fide*, because they informed us that they had been infiltrated and there was a lot of information being sought from other agencies pretending to be from an authorised source but were actually not. So although we think it is a good idea obviously to be opening up more, and to be sharing information for greater cooperation, we have to be aware that when we open the window, as Deng Xiaoping, a Chinese statesman once said – the flies also come in.

We want to have that protection which we have with the Attorney-General and some people might say that they need to do this in a hurry because sometimes we cannot delay these things. But because Fiji is a small country and we have a small jurisdiction, it actually works in our favour because we can coordinate very quickly. With the *Amadea* case, that was something we needed to act on very quickly. So, there was no delay at all going to the Attorney-General's Office - his people were able to authenticate the request with a quick call to the US Embassy. They knew people in Foreign Affairs - they can do all of that, the thing is signed off and the Authority to Proceed can go within hours to me and to the Police, and we were able to expedite the requests. There really is effectively no delay, in fact to date, all mutual legal assistance requests received by Fiji have been dealt with expeditiously, and in our view there is no reason they should not continue.

With the Juveniles Act, we note that the Cybercrimes Act has amended the Juveniles Act by Section 62(a) however, whilst the amendment defines to a greater degree pornographic activity in broader terms as it relates to children, it does not appear to criminalise the simple possession of child phonography on a computer. The possession of child phonography on a computer system would need to be included in a Juveniles Act or possibly as separate offence under the Crimes Act in order to conform to Article 9(1)(e) of the Convention. Currently the simple Act of possession of child pornography is not a criminal offence in Fiji.

In conclusion, Mr. Chair, in our opinion the Convention represents a progressive move towards the facilitation of greater international co-operation in dealing with cybercrime. It is our submission that Fiji should accede to the Convention with reservations to Articles 27(9)(a-e) and Article 31 as is allowed for under the Convention. It is also our submission that the Cybercrimes Act and the Juveniles Act require further amendments:

1. Cybercrimes Act should be amended to ensure that all requests from requesting countries go through the Attorney-General as they currently do under MACMA; and
2. the Juveniles Act should be amended to criminalise the simple Act of possession of child pornography.

Our final conclusion is that appropriate budgetary resources are allocated to the office of the DPP and other agencies in order to prepare for Fiji's accession to the Convention, particularly with respect to the 24/7 network establishment. Those are my submissions Mr. Chairman, thank you very much.

MR. CHAIRMAN.- Thank you Mr. Pryde for your elaborate submission on the Convention before us. You have dissected it, you have given us recommendations which is very forthcoming for the Committee in our final write-up of the Report. At this point in time, honourable Members, do you have any questions for Mr. Pryde?

HON. P.W. VOSANIBOLA.- Mr. Chairman on behalf of the Committee, I would like to thank Mr. Pryde for the submission this morning. As he had mentioned earlier on the focal point for cybercrime in relation to its difference with MACMA, so under the Cybercrimes Act, who is the current focal point on that if we are from another country wishing to dispose some case with us?

MR. C. PRYDE.- The central authority - the Attorney-General is still the central authority and that is preserved for a lot of the sections under the Cybercrime Act, but not all. And I note that if we, Fiji, were to make a mutual legal assistance to another country, we must do that through the Attorney-General and this should be reciprocated, so any law enforcement agency should go through the Attorney-General first. The Attorney-General's commanding authority under Mutual Assistance in Criminal Matters (MACMA), under the Convention and under the Cybercrimes Act is still preserved. Our concern is that it can be diverted and I am not so sure that this is a good reason for doing that. I know that when we were dealing with mutual legal assistance requests in the past, it was much easier just to deal with the Attorney-General's office.

We would know that they had properly assessed the request. If it does not go through them, it goes through the police. The police say to us we need to make an application in Court based on a mutual legal assistance request, we might have questions about the bona fide of who is making that request. And in any event, I will imagine either my office or the police would still want to go through the Attorney-General to get assurances on certain aspects of it. So that being the case, I do not see that it would hurt to simply make it mandatory for those requests to go to the Attorney-General in the first place and it also takes the pressure of the individual enforcement agencies having to make those decisions often in a very rushed manner.

MR. CHAIRMAN.- Mr. Pryde, on the subject of 24/7 we heard from the Fijian Intelligence Unit (FIU) that they were under-resourced but having to contend with the 24/7 arrangements so to speak. When you see your office moving forward, would your office be contentious with a 24/7 operation should the need arise and given the resources?

MR. C. PRYDE.- Yes, certainly if we were required to, we would with the budget that we have already got, we can always do that. With the *Amadea* we were all available so we are aware of our responsibilities so we can certainly do it. I suppose what we would be suggesting is a smaller increase so that we can deal with drivers for example. It is pretty more administrative staff that would need to be available 24 hours for the service of documents for example - that sort of thing. So the resourcing would not be a lot, but I would prefer to have some more to be able to deal with that if that was to go ahead.

MR. CHAIRMAN.- Thank you Mr. Pryde, as a Committee we will certainly keep that in mind when finalising our report. If there are no further questions honourable Members, Mr. Pryde I take this opportunity to once again thank you and your team for appearing before us this morning. Should we have any other further pressing questions or clarifications, we hope that you will accede to our request. With those few words, I thank you once again Sir.

The Committee adjourned at 10.50 a.m.

The Committee resumed at 11.01 a.m.

**Interviewee/Submittee:**      **Fiji Women Crisis Centre**

In Attendance:

- |    |                    |   |                        |
|----|--------------------|---|------------------------|
| 1. | Ms. Shamima Ali    | - | Co-ordinator           |
| 2. | Ms. Miliana Tarai  | - | Head of Legal Services |
| 3. | Ms. Stephanie Dunn | - | Legal Officer          |
| 4. | Mr. Semi Turaga    | - | Communications Officer |

---

MR. CHAIRMAN.- Ladies and gentlemen, before us this morning we have the Fiji Women's Crisis Centre and I give Ms Shamima Ali to introduce her team and continue with their submission, after which we will have a question and answer session.

MS. S. ALI.- Thank you very much. A very good morning to the honourable panel and to the administrative staff. I would like to introduce, on my left Miliana Tarai - the Head of Legal Services and Stephanie Dunn - the Legal Officer from our Legal Department and in the room also is our Communications Officer - Mr. Semi Turaga.

Thank you very much indeed, Mr. Chairman and the honourable panel for giving us this opportunity. I will start off with a brief on the Fiji Women's Crisis Centre and then my colleagues will continue with the different parts of the challenges to the Convention, with some recommendations, data, et cetera.

The Fiji Women Crisis Centre is a human rights organisation, based on the principles of human rights, democracy and the rule of law which has been in existence for over 38 years. The goal of the Fiji Women Crisis Centre is to eliminate all forms of violence, in all spheres of life, against women and girls in Fiji and the Pacific. We implement this vision through an integrated and comprehensive programme designed to prevent and respond to violence by reducing individual and institutional tolerance of violence against women and girls, and increasing available and appropriate services for survivors.

We address the problem of violence against woman using a human rights and development framework. This focus on human rights includes a feminist analysis of the problem and permeates all aspects of our work, recognising that the root causes of violence against women are unequal gender power relations, embedded in patriarchy. Violence against women is a pandemic that is globally recognised as a political, social and health problem. It is a grave violation of human rights.

In Fiji, 64 percent of Fijian women who have been in an intimate partner relationship experienced physical or sexual violence of both by their husband or intimate partner in their lifetime. This is almost double the global average. While efforts from Non-Government Organisations (NGO), State and other stakeholders have more than doubled in the recent past, it is evident that it still remains a crisis. One that is exacerbated by natural disasters, political upheavals and pandemics. The exacerbation of this crisis has now translated onto the virtual platform. Cybercrime is quick to occur and difficult to prosecute. Network intrusions and hacks can take place in a matter of seconds with complete anonymity and those that do leave criminal trails do so through a maze of computer infrastructure.

Information and Communication Technologies (ICT) have transformed societies worldwide and is now a lifeline for many, especially during COVID-19 restrictions/isolations (as we saw recently). However, ICT has also made societies highly vulnerable to security risks such as cybercrime. Appropriate safeguards and a unified effort nationally and internationally can assist in tackling cyber related offences.

The Convention on Cybercrime (Budapest Convention) can provide the framework that Fiji can use to strengthen its cybercrime legislations and policies. The Treaty's objectives are threefold:

1. Harmonising national laws related to cyber-related crime;
2. Supporting the investigation of these crimes; and
3. Increasing international cooperation in the fight against cybercrime.

We welcome this opportunity to assist the Standing Committee in reviewing the Budapest Convention and we commend the State for considering becoming a State Party to this Convention. This paper will review and discuss whether Fiji should become a State Party to the Cybercrime Convention, also known as Budapest Convention. I will now handover to Mili to talk about the challenges of the Convention.

MS. M TARAI.- Mr. Chairman, for the challenges of the Convention, there are two subtopics that we will be discussing, the first of which is the procedural safeguards. While it is sometimes referred to as the gold standard, because it is the most comprehensive multilateral Cybercrime Treaty, the Budapest Convention has been critiqued for not having stronger safeguards for human rights.

While the Convention lacks privacy and civil liberties protection, the procedural provisions are vague and also ambiguous. Consequently, this gives a lot of room for States to empower their law enforcement agencies to carry out acts that can encroach on the preservation of human rights and democracy. For instance, the surveillance powers that this Convention would hand to the enforcement agencies are not balanced out by the meaningful privacy or civil liberty restraints. Unlike other international law enforcement agreements, such as Interpol, Europol and Schengen agreements, this Convention does not include specific provisions to protect citizens' privacy. In fact, the word 'privacy' does not appear once in any of the Articles within the Convention.

Another example is the weak protection that the Convention has when dealing with political activities. The term 'political offences' is not defined and this ambiguity can be used to silence citizens and human rights defenders in our country. This poses a real danger to the spirit of democracy, human rights and the rule of law for our nation. Definitions are fundamental for the law uses definitions to separate the issues of fact from the issues of law.

Under the Convention, Fiji's assistance could be authorised in many cases solely by law enforcement, which can then be without judicial approval or oversight. Since the Convention does not even have a reporting requirement, that is, requiring instances of cooperation with other countries on foreign crimes to be made public, law enforcement decisions on this sensitive issue may never be subjected to civilian check or oversight. A lot of data can be collected and handed over to the foreign States merely on suspicion or if a person is being charged.

The threshold for the use of these powers by law enforcement is not properly defined within the Convention itself and this again poses another danger to human rights, the rule of law and democracy, as this power can easily be abused. Without proper safeguards in place, this Convention will empower law enforcement to carry out improper surveillance and unnecessary intrusions into the lives of our citizens under the pretext of cybercrime. Should Fiji decide to become a State Party to this Convention, then we urge that Fiji ensures human rights democracy and the rule of law be placed at the centre of the Convention, to avoid a one-sided application and enforcement in the future. In addition, having proper procedural safeguards in place, will also neutralise the threat to human rights and civil liberties.

The second sub-topic is that of gender. While the Convention is comprehensive and provides a coherent framework addressing cybercrime offences, the Convention does not take into account gender. Gender shapes and influences online behaviour and affects access to justice for survivor victims of Online Gender Based Violence (OGBV), such as cyber-stalking, revenge porn, sextortion, gender based violence, hate speech and the list goes on. Online gender dynamics strengthens and amplifies gender inequalities that already exists in the offline world. Cybercrime also impacts people based on their gender identity, however, cybercrime is not gender neutral and neither should our response to it be.

If Fiji decides to accede or ratify this Convention, then we urge that Fiji integrates a gender perspective in the implementation and enforcement of the Convention in our domestic context. This will help us to create effective laws, policies and procedures to efficiently prevent and combat cybercrime. We also urge that Fiji consider other conventions which offer more protection to women and girls such as the Convention on Preventing and Combatting Violence Against Women and Domestic Violence or fondly known as the Istanbul Convention, to work hand in hand with the Budapest Convention to ensure better protection for our women and girls and the recognition of online gender-based violence being a violation of a woman's human right.

I will now hand over to my colleague Stephanie Dunn to discuss the advantages of the Convention.

MS. S. DUNN.- Thank you. On the advantages of the Convention, as our paper discussed in regards to online gender-based violence, it takes many forms and is often intersectional in nature meaning that women from diverse and vulnerable communities are disproportionately and often severely impacted. Globally, rates of OGBV are increasing and with spikes being experienced during COVID-19 lockdowns and isolation, Fiji's experience was no different.

The Fiji Women's Crisis Centre statistics from the two centres showed that 51 cases of cyber abuse was recorded over a period of five years. It also showed that there was a steady increase in the number of survivors from 2018 to 2021. During the COVID-19 lockdowns or isolation, a dramatic increase was noted, so from 2019 to 2020 there was a 233 percent increase and from 2020 to 2021, another 40 percent increase was seen. The statistics also showed that survivors were predominantly women and over the years we have been receiving cases of cyber offences, however, we did not identify it as such due to the lack of legal framework that existed at that time.

Now women are disproportionately targeted to experience every form of online abuse. Online gender-based violence thrives where gender inequality is already well entrenched, is rooted in misogyny and is designed to control and silence women online. Now online abuse of women and girls is more violent, sexualised and is focused on appearance than online abuse experienced by men.

The United Nations reports that 73 percent of women online have been exposed to online abuse and that women are 27 times more likely to experience online harassment than men. The online abuse that younger women, ages from 18 to 24, experience often includes more dangerous forms of stalking and violence. Unfortunately enforcement agencies tend to minimise the severity of the online abuse, despite its very real physical and very real psychological consequences.

Most survivors of online gender-based violence just want the violence to stop and while others may want the person to be charged and prosecuted, some survivors may want to increase the security and privacy of their technology to prevent or minimise the abusive person's contact. It is very important to note that all survivors want the perpetrators to stop their harassment online, and any harmful posts to be brought down as soon as possible.

In the last quarter FWCC has noted a trend where harmful posts are taking longer to be removed from the internet. Reasons provided to us have ranged from law enforcers lacking the jurisdiction, to law enforcers being unaware of the law, to the expertise or resources that are needed to bring these posts down – not being available.

The Budapest Convention's primary focus is on crimes committed via the internet and other computer networks dealing particularly with infringement of copyright, computer-related fraud, child pornography and violations of network security. It does provide a framework that permits hundreds of practitioners

from State Parties to share their experience and create relationships that facilitate cooperation in specific cases including in emergency situations, beyond the specific provisions foreseen in this Convention.

The Convention could help build the capacity of countries with less experience in tackling cybercrime and provide the basis for technical assistance. This means, for Fiji, that we will have a network of experts to lean on in order to build capacity and provide expertise and resources when responding to crimes committed online. This is especially important for survivors of online genderbased violence, who need transparent and swift responses, as well as effective remedies.

Now, based on what we have provided in terms of the advantages and the challenges, while:

1. Fiji does have a Cybercrimes Act 2021 already in place, we do recommend that Fiji accede to the Budapest Convention.
2. Acceding to the Convention, the challenges noted above needs to be considered. It is high time that we start talking about the balance we want between our security and our privacy in the digital age. Investing in rights-protecting alternatives is the right way to go.
3. We do commend Fiji for considering to become a State party to the Budapest Convention, it is important to note that women and girls need far more than what the Convention can present. Therefore, it might be wise for Fiji to also consider other Conventions which offer more protection to women and girls such as the Istanbul Convention, to work hand in hand with the Budapest Convention to ensure better protection of our women and girls and the recognition of online gender-based violence being a violation of a woman's human right.

MS. S. ALI.- Mr. Chairman, Sir, that brings us to the end of our formal submission.

MR. CHAIRMAN.- Thank you Ms. Ali and the team for that comprehensive submission. You have dissected it into sections and you have particularly highlighted some of the challenges as being the safeguards and the gender issues, as well as the advantages of the Convention locally and also your recommendations. Honourable Members do you have any questions for the team?

HON. DR. S. GOVIND.- Thank you Mr. Chairman, Sir, and for a very comprehensive presentation. You recorded about 51 cases of cybercrime. So, what I would like to know is what sort of crimes were they and what actions were taken? Because you need good coordination with agencies such as the police and others to act on it, so in your experience how did you coordinate? What sort of responses were there?

MS. M. TARAI.- Now from 2018 and 2022, what we had noticed was in terms of imagebased abuse. Those were examples that we had seen survivors experiencing obscene publications, meaning that their nude photos or images shared with an intimate partner whom they had trusted and consented to give, was

then shared with the public once their relationship had broken down. Also included in the image-based abuse are those images where normal photos of a woman with her family, have captions pulling them down.

With regards to our cultural context in Fiji, reputation is very important for our young women. For a lot of them, these photos may seem like a normal photo but the caption itself breaks down their virtue, talks about their appearance as well as the types of family values that these family members are instilling into her.

Apart from that we have also notice tracking - trying to find the survivor's location, especially for intimate partners - they could be husband and wife, *defacto* partners or boyfriend and girlfriend - tracking where they are going, how long they are in that particular place, also tracking their *Facebook* accounts, who they are speaking to, the friends that they have and their messages. We have also noticed stalking online where they may not have any relationship at all but they are stalked online through their *Facebook*, *Instagram* and *Twitter* accounts.

One of the difficulties that we have seen when they do go out for help is (like we have said in our submission) that the violence is minimised. The comments that we hear from enforcement agencies is "Well it is online, it would not hurt you that much. I think the best thing for you to do is get offline". But the difficulty with that is that when you are removing them online and putting them offline, you fail to understand that whatever is happening offline, is translated onto the online platform. So, it does not reduce the risk for her, it just also amplifies the risk for her because there have been instances where the perpetrator cannot locate the survivor online, they go to the survivor's workplace or to their homes.

We have also seen instances of doxing where they place a woman's private number or home address on porn sites, asking for or soliciting sex saying that they are available. Others have been hired to come in and install maybe lights or security systems, but instead they are installing cameras then the images that they illegally get from these cameras are then shared putting the survivors' lives at risk. And even worse, it takes even longer for the survivors to get the assistance that they need. I will just handover to the rest of my members if they want to say something else.

MS. S. ALI.- It is also used for blackmail like the one that Stephanie was talking about, where people come in to install other things or come and change the locks and they install cameras, then they threaten the woman and say that they have got these images. They will send her a few and you know she is going about her daily business in her own house and so on but she may be half naked or coming out of the bathroom and things like that. They can threaten her and say that they have got more and if she does not show them anymore or send them more intimate pictures, then they will release the ones they have. They can say, "Come and have sex with me and meet me here", et cetera, so all those things are threats.

Also in domestic violence cases, we have cases where the woman has decided to leave a violent relationship, so he has got pictures of her from before when they were lovey-dovey and so on, and he is now threatening to put all those things out in the public if she does not come back and things like that - we are also getting more and more of that now.

As far as law enforcement is concerned we do work very closely with the Police but we have put down the reasons why they do have the technology. I will tell you the story of one young woman. Six, seven years later she still has not had any justice and she knew who the suspect was, who had come in to install whatever and we went, she was given the run around to come to Suva because the Cyber Unit was here, CID and eventually someone pointed her to us and we started working with her. She went back to the town she came from and the guy was sending pictures one and by one and so on. Till today nothing has been done. Our Police Liaison Officer has been going around to the Police Station to ask what happened to that case, but the woman has now given up. People give up and these people continue to harass other women because the justice has not been done.

I am sorry that I could not bring any of our counsellors today because they were also busy, but they will have more stories to tell. They have a lot of issues with law enforcement on this and that is why we are talking about strengthening the laws and particularly paying attention to the gender aspect of cybercrime.

HON. DR. S.R. GOVIND.- Does the Centre have capacity in terms of technology to carry out some surveillance?

MS. S. ALI.- We do not have that and we do not have the resources. Our young ones are very tech savvy so we do not see that as our area of work, you know we have got law enforcement and so on. We have Stephanie and other staff but Stephanie leads our Cybercrime Against Women team and she is also part of the Online Commission. She belongs to a Committee there so trying to work through them also but we do not have that.

MR. CHAIRMAN.- Certainly, the roll-on effect from that is what you said about that case of six or seven years and she has given up - it leads to possible suicide and there is a high degree of suicide that eventuates from these things. Just to touch on, honourable Doctor Govind about resourcing particularly, are you a 24/7 organisation?

MS. S. ALI.- Yes, we are, since our inception in 1984 but now for the last five years, the Ministry of Economy contracts us on a budget of \$200,000 to run the toll-free 24/7 line which is 1560, so we are running that also for Government. All our services - the counsellors, the lawyers - we are all on 24/7 alert.

MR. CHAIRMAN.- That is very good to know, I think we need to push up your request for additional funds.

HON. S. ADIMAITOGA.- Through Mr. Chairman, actually I really appreciated your submission this morning. You have urged that Fiji consider other conventions like the Istanbul Convention which I believe is closely related to the Budapest Convention; can you elaborate further on this Istanbul Convention as you have stated that we should touch on other conventions?

MS. M. TARAI.- The Istanbul Convention focuses primarily on combating violence against women. What the Istanbul Conventions says is that it is the State's responsibility to prevent all forms of violence against women, protect those who experience violence and prosecute perpetrators. The Istanbul Convention also provides avenues and mechanisms for the States to actually go back to their different countries and ensure that domestic legislations are set up to also allow room for compensation, for the survivors. Because so far, what we are seeing is that when we have survivors of central or domestic violence, they are not compensated because it is not within our legal framework.

The Istanbul Convention actually allows for survivors of gender-based violence or women who undergo violence, to actually have room to ask for compensation and the offender or the perpetrator will then compensate them on those things. It also provides a lot of mechanism for security for women especially survivors as well. It is very comprehensive and actually promotes equality between men and women, and the prevention of violence against women is encouraged through mutual respect, non-violent conflict resolutions, questioning gender stereotypes as well (which is very important) and it also includes all these through teaching materials in schools. So it starts from the very grass root level - from school levels all the way up.

It also allows the State to investigate allegations of violence and prosecute the perpetrators and the State must also protect and support those who had experienced violence, as I was saying, by way of compensation. It also tell the States to look into avenues of providing long term accommodations for survivors of violence as well, to protect women. The Istanbul Convention is primarily for women.

HON. DR. S.R. GOVIND.- One key thing to prevent Cybercrime is to educate women, does the Centre have an educational programme? If it does then, how do you develop your educational programmes? This is such a complex technological issue so how do you educate women in your groups?

MS. S. ALI.- Thank you for the question honourable Member. Yes, definitely we have a lot of education programmes and the demands are quite high, particularly in the rural areas and we also go on requests from other organisations. We are now beginning to include this into our manuals like the Gender Violence against Women's Rights Manual - something like that. But we have already started talking about this to women; the risks that they run and so on, through online violence and things like that. We are doing that already and we are including that now in our training manuals. It is quite complex and we are not ICT experts, but Stephanie and her team are also in touch with people and she can explain that.

MS. S. DUNN.- Sir, we work closely with the Online Safety Commission as well as E-Safety Commission in Australia. They have also provided a bit of training as well and we are also working quite closely now with the Attorney-General's Office for Australia to try and tackle cybercrime not only here but also in the Pacific. One of the things that we have seen in terms of our community awareness is while we talk about risks, we also talking about how best to protect themselves. For those of us that say screenshot is an easy thing to grasp and that everyone understands - not everyone does because everyone is under the illusion that once it is there online it will be there forever. Sometimes when a person does remove it, it makes it very difficult for law enforcements to then collect evidence in those particular cases. In these things we teach them how to better protect themselves online and who to go to. Let us be honest - a lot of people do not understand or know what online violence is and they do not know the forces that they should go and report the matter to.

HON. DR. S.R. GOVIND.- If someone is trying to send some irresponsible messages to you, one simple thing is to just to block that sender then you will not receive the message? Do women know about this?

MS. S. DUNN.- The difficulty is, like we had pointed out in our submission, blocking the perpetrator does not necessarily mean that the violence will stop. What we have seen is that once you block this account, the perpetrator can make another fake account and then send you messages. And if that does not work they set up a fake group and then they bring your name down in that group, and if you bring that down that, the cycle continues. The main issue is just to target and educate one but also target the mindsets that fuel it. That is why we were talking about patriarchy and about unequal gender relations - that is very important to understand.

In terms of online violence, we do not necessarily tell survivors to get offline because it is equally their right to be online and enjoy that platform, that is their lifeline. During COVID-19 it proved to be such a valuable lifeline for a lot of women - they were able to contact their friends, their families. What is very important is that they are able to use it safely and we just show them a few tricks to keep them safe while at the same time, ensure that the perpetrator is brought to justice. But one very key thing we always say is that it is not the survivors' duty to prosecute. It is her job to stay safe and it is not her job to collect evidence. A lot of survivors coming forward are saying that the Police Officers or the enforcement agencies are asking that they collect evidence and give it. It is very difficult for a survivor to do that. What we do as part of our programme is to also educate them on how to stay safe online, and what they can do to lodge a complaint and that also includes the platforms itself. Where they can lodge a complaint on the platform if it is violating their terms of conditions and how they do it.

MS. S. ALI.- I just wanted to respond to what was said earlier about being suicidal. Most of these women particularly when their pictures have been posted in comprising positions, half clothed, not clothed, et cetera that is a great sense of shame to them because the families and everyone is affected. Most of these women - where those kind of things have been done - are suicidal when they come to us.

HON. S. ADIMAITOGA.- Mr. Chairman, through you, while reading through your submission this morning, you said that without proper safeguards in place, the Convention will empower law enforcements to carry out improper surveillance and unnecessary intrusion into the lives of citizens under the pretext of cybercrime. What I am coming at is this; should Fiji decide to become a State party to this Convention, you have urge Fiji to ensure that human rights, democracy and the rule of law be placed at the centre of Convention to avoid being one-sided. Can you elaborate further on what you said about avoiding one-sided applications on enforcement in future?

MS. M. TARAI.- What we were explaining in our submission is that the Convention gives so much power to law enforcement agencies, so there is no oversight, no checks to that and there is no sense of balance that the Convention talks about. When you put human rights, democracy and the rule of law at the centre of the Convention, you will be able to see how the people are going to be affected. So when it is translated on to our domestic legislations, we are able to also ensure that while we give the enforcement agencies these powers, human rights of all the citizens, the rule of law and the concept of democracy should remain. That is what we were trying to explain in our submission. If you have proper procedural safeguards in place, it will neutralise the threat to human rights, rule of law and democracy.

MR. CHAIRMAN.- Ms. Ali and the team from FWCC, I take this opportunity on behalf of the Committee to sincerely thank you all once again for availing yourselves, and should we have any other pressing questions or queries that you will avail yourself in the not too distant future.

MS. S. ALI.- I would just like to thank you very much, honourable Members. We know we were not in the list of organisations asked to submit, but we did catch some of these on the national TV and decided to request and it was acceded to so thank you for giving us this opportunity. Definitely, we will be available for any further questions or clarifications. *Vinaka vakalevu.*

The Committee adjourned at 11.37 a.m.

**[VERBATIM REPORT]**

**STANDING COMMITTEE ON**  
**FOREIGN AFFAIRS AND DEFENCE**

**TREATY/CONVENTION**

**Budapest Convention on Cybercrime**

**INSTITUTION:** (1) Fiji Revenue Customs Service  
(2) Bank of South Pacific (BSP )

**VENUE:** Big Committee Room (East Wing)

**DATE:** Monday, 17<sup>th</sup> October, 2022

**VERBATIM NOTES OF THE MEETING OF THE STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE HELD IN THE COMMITTEE ROOM (EAST WING), PARLIAMENT PRECINCTS, GOVERNMENT BUILDINGS ON MONDAY, 17<sup>TH</sup> OCTOBER, 2022 AT 10.05 A.M.**

**Interviewee/Submittee:** Fiji Revenue and Customs Service (FRCS)

**In Attendance:**

1. Mr. Tevita Tuiloa - Investigation Compliance and Intelligence Unit
  2. Mr. Edward Eterika - Legal Unit
  3. Mr. Kele Gukirewa - Customs Border Team
  4. Mr. Robert Khan - Deputy Director Information Technology
  5. Mr. Ryan Prasad - Technical IT Unit
- 

MR. CHAIRMAN.- Honourable Members, members of the public, secretariat, ladies and gentlemen a very good morning to you all and it is a pleasure to welcome everyone to this submission this morning. For your information, pursuant to Standing Order 111 of the Standing Orders of Parliament, all Committee Meetings are to be open to the public, therefore, please note that this submission is open to the public and media, however, due to some technical difficulties this session will not be streamed live on Parliament's website and social media online platforms and the Parliament Channel on the *Walesi* Platform. Allow me now to introduce my Committee Members.

**(Introduction of Committee Members)**

With those few words, I welcome the team led by team leader Mr. Tevita Tuiloa - a brief introduction by your good self then you can start your submission after which we will raise questions. The floor is yours, Sir, thank you.

MR. T. TUILOA.- Thank you very much Mr. Chairman of the Standing Committee on Foreign Affairs and Defence, good morning honourable Members, on behalf of the Chief Executive Officer for Fiji Revenue and Customs Service, thank you for inviting us to come and make our submission on the Convention on Cybercrime (Budapest Convention) given the rising tide of cybercrime across borders and also here in Fiji.

**(Introduction of FRCS Officials)**

Thank you very much honourable Committee Members for giving us an opportunity to send our submission on the Convention on Cybercrime. Sir, by way of an overview of our presentation, we will be discussing a bit about the functions of FRCS in terms of tax and customs. As this is a Convention on Cybercrime, we will also be discussing a bit about the confidential information and sensitive data that we normally receive by way of the performance of our functions. We will also be discussing our submission on the review of the Cybercrime Conventions and applicability to FRCS; the challenges that we perceive we will face upon ratification of this Convention; the way forward that we can also consider; and our conclusion on the same.

The functions of FRCS is captured under Section 22 of the FRCS Act. The functions are that we act as the agent of the State in providing services and administering and enforcing customs and tax laws. Also we have the function of disbursing loans or funds on behalf of the State. We exercise all functions and perform all duties necessary for the collection and recovery of tax or customs duties. We also advise the State on matters relating to taxation, customs and excise; represent the State internationally in respect of matters relating to taxation, customs and excise, and we also perform other functions as the Minister may assign to the Service.

While we are performing our functions as required under section 22 of the Act, obviously we will be receiving very confidential and sensitive information. Just to inform the Committee - we have a specific section in our Act, section 52 of the Fiji Revenue and Customs Service Act which protects any confidential information or documents that we receive from taxpayers, travellers or traders while in the performance of our duties. In terms of confidential or sensitive data that we receive, either through physical or electronic means, firstly, we have personal information. We have a volume of personal information on taxpayers, travellers or traders which include their residential address, bank details, passport and information of their personal assets, we have all that information.

In terms of companies, we have the company financials, their profit and loss statements and their shareholding structures, information pertaining to the companies themselves in terms of importation - the importers, and we have importation and exportation data. We have Single Administrative Document (SAD) entries and these entries are submitted when it comes to importation or exportation. This information contains sensitive information such as Bill of Lading, invoices and information of the suppliers that are providing these goods that are imported into the country. We have those information as well.

In terms of information we also have data on foreign companies and entities that we have been able to receive through information exchange through Double Taxation Agreement (DTAs). We also have other data which we acquired over the years whilst performing our functions under our customs and tax laws. These are the volumes of information that we have that are confidential or sensitive. How did we obtain this information? We have the usual lodgement of returns by the taxpayers, for tax purposes - these are the income tax returns, VAT returns, and other types of tax returns. We also have the lodgements when it comes to importation of SAD entries, IM-4 entries and IM-7 entries. These are the types of information we receive through customs.

In terms of other sources of information, we have obtained them through our administrative notice. Administrative notice is the power that we have to provide a notice under section 36 of the Tax Administration Act to third parties when we want to acquire information on a particular taxpayer, so we use the administrative notice. Also, we have seizure provisions under section 35 of our Act, and section 129 of the Customs Act. Under seizures we are able to secure certain confidential and sensitive data, and obtain such confidential information through exchange of information by way of DTAs or obtain them through MOUs with the relevant enforcement agencies both regional and local. Sometimes we normally get these information through voluntary means provided by the taxpayers, travellers or traders themselves. We agree that with the information that we have, there is a need to ensure that there are legislative and other measures in place, to ensure that such confidential information is protected.

Moving onto the reviewing of the Cybercrime Convention and its applicability to FRCS. The team has looked through the Convention and we have only highlighted a few, which we wish to make submissions on. We have looked at Articles 4 and 5 and these two specific articles discuss data interference or system interference, where it should be made a crime if someone tries to sabotage, alter or destroy any data information. In our specific tax and customs laws, there are no actual specific provisions where we will actually prosecute a taxpayer or an importer for damaging or altering such electronic data or computer system. We wish to recommend that we have such powers in our legislation as well because we all agree that data especially in terms of tax purposes, is an important data that needs to be safeguarded and if a specific taxpayer or an importer wilfully tries to damage such information, we should hold them accountable for those actions as well. That is one of our submission for Articles 4 and 5.

We have also looked at Article 9. Article 9 talks about offences relating to child pornography. One of the functions of FRCS is border protection to ensure that any such malicious activities is kept and controlled at the border and not introduced into the country. We feel and agree that child pornography is one such malicious activity that should not be entertained here in Fiji. We are proposing that there be such legislative powers to enable Customs officers to work closely with our fellow enforcement agencies such as immigration and police officers, in detaining any computer data storage medium which has child pornographic content, at the border on reasonable grounds.

We have a specific provision in our Act under our CPIER so that is the Customs Prohibited Import and Export Regulations. This particular power only allows us to detain anything or any material that has any pornographic images on it. It is not really specific in terms of child pornography but it covers as a medium for any type of material that is explicit, that is not wanted in Fiji. We can detain that. Perhaps we can have powers alongside that to enhance and specifically cater for child pornography as well.

Moving on – we have also looked at Article 10 which talks about offences relating to infringement of copyright, IPR at the border - copyright and related rights. We have suggested or proposed in our submission that ex officio powers be granted to Customs officers to detain and destroy any goods that is

in breach of any IPR laws that we have identified at the border, which may have been procured by the importer, by means of a computer system.

Just for the Committee's information, we have also looked at the current Trademarks Act of 2021 and we have noticed that the Act itself has made specific powers in each section that is basically ex officio powers, that allows custom officers to detain and destroy any goods that is in breach of IPR laws at the border. That Act has already covered it but as we are aware, the Act is yet to be enforced as well, so probably this is one of the articles that already has a way forward in terms of its solution.

Looking at the next Article, Article 19 talks about search and seizure of stored computer data. Just to inform the Committee members, FRCS has powers specifically under sections 35 and 36 of the Tax Administration Act, to furnish, seize or detain any electronic data and any electronic data storage device for administering our tax law, so it is only for administering our tax law only that we are allowed to detain any electronic data or electronic data storage device.

We have also noticed that there are no specific powers for our Customs officers under Section 129 of the Customs Act to detain electronic data or electronic storage device. We have powers to detain goods but not specified specifically to electronic data or the storage device itself. So, for us we view that as something we can work on if we are to also ensure that Article 19 is maintained.

The last submission is on the whole of Chapter 3. We have actually gone through each of the Articles and just a point of concern on international cooperation in terms of data sharing. There are quite a lot of Articles relating to that and for us we feel this is an issue because of section 52 of the FRCS Act which deals with secrecy provisions of maintaining confidential information. The Act limits how we actually share the data that we have. The limitation is that we need to have a Memorandum of Understanding between us and the enforcement agencies that will be relying on the data; and that the information we share is to be used specifically for the performance of that enforcement agency (their functions) that is the only way we can share the information to them.

Our concern is that when it goes cross-border wise, when an international entity or organisation is involved in this information sharing. The understanding is that this information is only shared between us and the relevant agency that is requesting - it is not to be shared to a third-party unless that third-party is acknowledged in terms of the MOU that we signed with them. That is just one of the limitations that we have in our actual section 52 itself.

The challenges in terms of the Cybercrime Convention - as we have already highlighted, our current legislation allows FRCS to only obtain data for exercising our powers in administering of tax, customs and excise laws only. We do not have any specific sections that deal directly with cybercrime. Furthermore, as I have explained earlier, section 52 limits FRCS capability to share information for the

purpose of combatting cybercrime in Fiji where certain conditions have to be met in order for the information to be shared to the relevant enforcement agency.

Lastly, in terms of monitoring and enforcement of cybercrime, FRCS requires continuous enhancements of the technology we have. At the moment we have just the bare minimum technology to monitor and combat cybercrime. We do not have the latest updated technology to be able to detect or combat any of these latest cybercrimes. Our proposed way forward on that is to consider amending our existing legislations - Customs and Excise, and Tax legislations to ensure that we are complying with the requirements under the Cybercrime Convention. We also propose that more training opportunities be provided for our staff members in terms of identifying, monitoring and combating cybercrime, probably looking into enhancing our current technology to be able to identify, monitor and prevent cybercrime; and also proposing more collaboration with other law enforcement agencies who are responsible for handling cybercrime issues in Fiji.

All in all, our conclusion is that FRCS supports the ratification of the Cybercrime Convention. Thank you. Are there any questions?

MR. CHAIRMAN.- Thank you Mr. Edward and the team for your overview on the subject matter, the Budapest Convention. You spoke about the functions, the information and data, lodgements, you gave examples of that and the different Acts, a dissection of the Conventions and how it relates to FRCS, the challenges and also the way forward. You also mentioned about the legislation.

Have you as an entity not put that forward to Government for these legislations to be looked into or amended?

MR. E. ETERIKA.- Just to answer the question, I think after going through the Cybercrime Convention we felt that there were a few areas which we could tighten up on our legislation obviously from the upcoming budget submission. We will be making proposals to ensure that our legislation is more specific in relation to those cybercrime offences and combating those. At the moment it is a bit wide and but it would be good to just have a more specific or targeted legislation on cybercrime activities.

HON. DR. S.R. GOVIND.- Thank you for your presentation. I would like to know whether if there has been any incidence of people committing cybercrime using the data you collect or do you have a surveillance mechanism to detect cybercrime?

MR. R. KHAN.- To answer that question, we have systems that can detect intrusions and systems that can prevent intrusions but they are regularly monitored but for cyber, we normally get that stopped at the door. It is an unseen element, but over the years we have subjected FRCS to what you would call Security

Penetration Tests - that identifies the gaps that exist on our network infrastructure but also on our applications that are exposed to the internet.

The results of those reports identify the high critical medium low gaps and from that we address the critical and high which is of priority. That is governed by our Audit Risk Committee and also our Board from which we then enhance the technology. As you know, the FRCS Tax System has gone online as opposed to the past when it used to be in-house based. So, having the tax system exposed online has brought about further improvements or the room for improvements that FRCS needs to move up to.

We also adhere to the industrial framework ISO270001 which enforces the information security management system. We are not there yet. It is a journey but we have made active improvements I would say, over the last three years. Further to that, there is something also called the Data Loss Protection. There have been instances in the past that you might have seen snapshots of, appearing in different areas on the web so to combat that, we are working on a security feature which is call Data Loss Protection and that basically helps identify the source of the information, where it is going, is it going to the right person and also tagging it whether it is only for internal use, classified, unclassified or public use.

I think that is a project that is to be delivered in this financial year. There is a lot for FRCS I guess with the different means of exchange. We are sharing data with third parties or the other stakeholders - FNPF, LTA, and government - so this is another thing which technology is moving into. You might have heard of the hack by Optus. In the last few days, one of the banks' hacks starting to come in from what you would call an Application Programming Interface (APIs) - these are like your gateways. So, if I talk to this party or that party I need to make sure that my gateway is secure and there are no gaps there. You always regularly identify the risks that come with that because the cyber risks are always evolving. You know six months' time there is something new there and then we have to increase our level of protection.

Once upon time there was Ransomware, so we have mechanisms to protect FRCS data for Ransomware, but there are things also like crypto currency - that is new and not easy. You have malicious forces trying to use your web service for mining and you will not even know - that is a new threat we have identified. We have put in some new investments to help protect our core systems around that, but it is always being on the watch (I would say). Security is also a large portion of our IT budget, just because of the data that we retain for tax, customs and also border. I hope that answers your question Sir.

HON. S. ADIMAITOGA.- Through you Mr. Chairman, to the submittee, Article 5 says that each party shall adopt such legislative and measures as maybe necessary to establish its criminal offences under its domestic law when committed intentionally. Do you have something up your sleeve that you can explain further into this - do you have it with FRCS?

MR. T. TUILOA.- Article 5 relates to system interference. This is probably in terms of the computer system itself, not the data but the actual computer system. So for us, our Acts specifically discusses about seizing information or even the storage device itself but only for tax purposes - just administering our tax powers. If we find out that the computer itself is in breach of any Cybercrimes Act, we will probably hand over to the police or the relevant enforcement agency that will handle it. Our only concern is that in our Act, we will only be handling the computer system if it is a breach under our tax laws.

For us, our limitation is the powers that we enforce - we have the ability to detain that computer if it is only for tax purposes or if there are any returns or any information inside that might be related to our line of work. But if it does not have any of that even though the computer might be in breach of a possible cybercrime, we do not have powers to detain.

HON. DR. S.R. GOVIND.- If someone is carrying a computer across the border, you do not have powers to stop and check what is in the computer, right?

MR. T. TUILOA.- As mentioned, we do not have the powers right now to even go through that computer unless we receive information - we will only stop people and their cargo and refer it for further police intervention.

HON. DR. S.R. GOVIND.- Does any agency have that power to check?

MR. CHAIRMAN.- Not unless they have been alerted from the departing country, only then can they apprehend them.

MR. T. TUILOA.- So that is the limitation in terms of our powers. Only if we receive an alert or tip-off from the relevant enforcement agency that a person is bringing in a computer or storage device that has specific information then we can detain him, but we will not be able to arrest the person. We do not have arrest powers, so we can only detain and refer to the relevant agencies that has the powers to deal with that, so normally it is the police. We do actually do risk compliance but when we get the tip-off, that is the main point that we can act and exercise our powers just to detain him while we wait for the relevant agency to come and deal with him specifically. Those are the limitations in our powers since we only act according to whether it is a customs or tax purpose issue.

MR. CHAIRMAN.- Honourable Members, if there are no other questions, it has been very interesting talking to the team from FRCS and at this juncture, on behalf of the Committee, I wish to thank you and wish you a blessed day and success in your endeavours to control cyber and its crimes so to speak. If you have any departing comments, the floor is yours.

MR. T. TUILOA.- On behalf of the Fiji Revenue & Customs Services I would like to thank the honourable Members and the Committee for giving us this opportunity to come and make our presentation. Obviously there is a big threat in terms of cybercrime, everyone has access to internet and our systems are always at risk. I think it is also an opportunity for us to strengthen our working relationship with other law enforcement agencies and work hand in hand especially with our other counterparts from overseas, in terms of receiving those tip-offs and risk profiling sharing mechanisms that we can use. But should the Committee have any further questions, you can always let FRCS know and we will try our best to answer. Once again thank you very much and we wish you the best.

The Committee adjourned at 10.36 a.m.

The Committee resumed at 11.00 a.m.

**Submittee/Interviewee:** Bank of the South Pacific (BSP)

In Attendance:

Mr. Omid Saberi - Chief Information Officer

---

MR. CHAIRMAN.- Mr. Saberi is the Chief Information Officer from BSP - a very warm welcome, Sir.

(Introduction of Secretariat Team)

With that brief introduction you may proceed with your submission after which we will have questions.

MR. O. SABERI.- Thank you very much, Mr. Chairman and honourable Members, it is a privilege to be here and thank you for allowing BSP to present its submission to yourselves. I am just trying to gather myself, I was just rushed in, so there was some confusion in regards to the time of coming to the Committee.

We are obviously in the technological age where information flow of data, financial transactions become permeated into everything we do. Just as technology has helped us traverse our boundaries by flying from place to place, when considering hundred years ago it would take a weeks to go from one place to another. With the same speed technology has also helped us send information across, nothing new for yourselves to know of course. But this ability has also given a new arena to those who want to defraud us especially financial institutions, because borders become almost irrelevant with technological advancements, those who can be sitting anywhere in their rooms or in their bedrooms somewhere and trying to defraud someone in Fiji or elsewhere, without any legal arm reaching them and then feeling comfortable in those areas.

So, especially for a financial institution like BSP, the cost of cybercrime is a growing concern. We have to constantly be on the front foot because no matter what we do, there are criminal who would almost find a way and find a loophole, so we cannot do it alone. If we try to do it ourselves we cannot, so it has to be a concerted effort, not only within the financial institutions but all the other arms available to us.

If you look at our submission, the global cost of cybercrime you can see it is a 15 percent growth in terms of financial cybercrime every year - year to year it is a 15 percent growth. In 2015, cybercrime cost the global community US\$3,000,000,000,000 and it is expected that by 2025 it will reach \$10,000,000,000,000 but right now in 2021 (right now like a couple of years ago) was \$6,000,000,000,000. To put it in perspective, if \$6,000,000,000,000 was the cost of cybercrime internationally and globally, and you consider that to be a country - it would be the third biggest economy after China and USA. That is just the cost of cybercrime to the global economy which basically takes away taxes, takes away people's funds that they could be using in other ways and it brings things like poverty in many instances. So this global movement to try and curtail or be able to manage this growing menace, is really very worthy. Surely for a small developing island country like Fiji, utilising the means available to it globally would be of great importance. We might be an island but surely from a global community we can be part of that global community and try to be connected to them rather than trying to be away from them. So immediately, that brings some benefit that we can think of. There are other benefits. There are frameworks in place that we can utilise, experiences are shared across the parties. Although Fiji may not have been part of the initial negotiations done, I think in 2001, when it was put together, but surely now there are committees that evolve it further, the Cyber Convention Committee, but immediately Fiji can be part of that and help shape the sooner we get onto it to shape the direction which it takes, because information technology moves very quickly. The cost for us in the Bank is to make sure that we are safeguarding the financial information - the customer information is enormous, and it is growing drastically year by year. There is cost to that, so being on this Committee, immediately Fiji will have some say in shaping some of the directions towards what would benefit Fiji a bit more.

Also, ratifying this Convention allows us to build capacity. Again they do have Cybercrime Programme Office, which again, Fiji can hook into and build capacity to manage. Being in the financial institution, we see lots of very creative ways that these conmen con our customers. I will tell you a few cases where at some point Fiji was targeted by criminals, especially from Eastern Europe, where they would come and scam on ATMs - I am not sure if you are aware of this. They would basically put readers on ATMs and read cards of customers and then they would replicate these cards and be able to utilise them on our ATMs.

If you look at our cards now, they have these chips on them - we did not have international cards and we did not have these chips, they were like without chips. So when the criminals realised that Fiji was not up to standard and they are not reading chip cards but will only read the magnetic stripes (magstripes) that means they can just swipe this. This is not as secure as this (Mr. Saberi pointing at the magstripes and the chip on the ATM card), so they were scamming cards all around the world and we have caught on. In fact, through the videos at our ATMs, someone had many cards and was just putting the cards in, and they were withdrawing hundreds of thousands of dollars from the ATMs - until all the banks in Fiji got their act together and we made sure that we did not only just accept magnetic stripes. You have to have chip cards

for us to accept it or we will reject it. So immediately, the criminals figured out that Fiji was now not a target anymore, because now they have upped their act.

What I am trying to say is that being part of a global community gives us the ability to keep up with technology which allows us not to become a target country. Once that happens, then financial institutions around the world will say, "Fiji is high risk and our cards will not be allowed to be used in Fiji." When that happens it immediately affects tourism and the country because you are considered to be a country that is out of the financial grid. So it becomes important that we are in the forefront with the global community in trying to meet that requirement to be fighting these cyber criminals in terms of financial fraud. Without financial access, the country will be hampered in terms of progression. Who knows in the future there might be a time when the bank institutions say, "If you are not part of this Convention of cybercrime, we will not allow you to transact in the country because you do not have the frameworks in place that allows us to find a criminal who is trying to traverse your financial systems. We are also safeguarding for the future.

There are some considerations as the submission says, in terms of privacy and civil liberties and in terms of dual criminality - something that might not be a crime in Fiji but it might be in some other country, it might be and how will we manage that. The Cybercrimes Act to some extent, addresses this, but there still needs to be some consideration around that. Fair use in terms of intellectual property is a bit vague - what is fair use of intellectual property and how we can look at that and of course to meet all the requirements of the Convention, the costs and the time, the parties and the stakeholders need to be given ample time to deploy them.

There are some considerations but overall, as a financial institution, BSP thinks it is only to our benefit to be part of this Convention - not only because it builds our capacity or gives us access to what is happening on the forefront of fighting cybercrime, but it also allows Fiji to have a say in the global community in terms of this important aspect. This is not going to stop, this is going to go further and further and tracking them is going to be even more important - everything. With internet, everything is going to be on the internet sooner or later, so the more provisions we have in place as a global community fighting it and putting in safeguards the better, so for sure we would want Fiji to ratify and be part of this Convention. Thank you and that is in brief, the submission.

MR. CHAIRMAN.- Thank you, Mr. Saberi, for your very insightful contribution to the Convention at hand and you have given us some insight of the banking fraternity so to speak. With those few words, honourable Members, do you have any questions for Mr. Saberi.

HON. P.W. VOSANIBOLA.- Thank you, Chair, through you. Just a simple question. How often do you face up with the cyberattacks on your financial transactions system?

MR. O. SABERI.- It is a constant fight (if I may use that word) because as soon as we put our systems available internationally, immediately we have a constant attack. For example, it is very important to keep these 16 digits on your card to safeguard it and not give it to anyone because when they know this number, they can basically try to access your funds. But we safeguard these and these are not sequential and these are called bins - bins for bank, okay. If we have overnight, a bin attack for example, where a fraudster will try different numbers, trying to find the right number, will try different combinations and suddenly we might have \$10 requests for 500 numbers - that will hit our system. Maybe one of them will work and once they figure out that the number is active or valid, then they will try to withdraw a thousand dollars online. So, we have to put different systems and safeguards, so sometimes when you try to do online, you are asked to put a one-time password. That is really to stop people from doing bin attacks - trying to by chance, figure out a number and take the money out.

We have put safeguards in the system that if it goes beyond a certain sum, you might be asked to put your one-time password, you will get it on your phone and you have to input it and different mechanisms that we do, so from a card access point of view, yes because this is available. If someone goes overseas and uses it in some ATM that has a card reader on it, immediately they will be attacked soon after. It is a constant vigilance that we have to have. Sometimes, as a BSP customer or any bank customer, you will be asked to change your card because someone has compromised it, and we even put provisions in our accounts because we know a certain sum will be lost to these sort of attacks. It is not the customers' fault so we obviously pay back the customer even if a customer loses a thousand dollars, we pay them back. It has nothing to do with them. It is these fraudsters trying to attack us, so it is a constant.

HON. DR S. GOVIND.- Thank you for your presentation. This requires a 24 hours surveillance - do you have a mechanism for 24 hours surveillance? Because other banks will also have the same problem. Can the surveillance system be shared across the banks? Is there some mechanism to consult other stakeholders?

MR. O. SABERI.- Yes, it is a layered approach. That is what I am saying, partnership becomes a very important part of this in safeguarding our systems. We can think about it like this room - we have doors that can be locked, then you have the perimeter and you have the policeman sitting there. You have a layered approach of security, so in the same way BSP will have its own doors and safeguards.

But then we also work with Visa which is global and they have their own standards. They also have their system because when we request for money or when a customer comes and asks for a service, let us say an overseas customer, we send it to Visa then Visa has its own checks - another layer of checks. They might stop it and say that the card is already a hot card so they might stop it, they might have a different provision. Then the other bank will have its own mechanism to safeguard and also we share information with each other - when we have something that we think is suspicious we also inform the other banks, so we have a layered approach for security, just like we have physical security.

MR. CHAIRMAN.- Honourable Members any further question for Mr. Saberi? If not, I take this opportunity on behalf of the Committee to say thank you for availing yourself. If we have other pertinent questions, grateful if you will avail yourself to those but if you have any departing comments Sir, the floor is yours. Thank you.

MR. O. SABERI.- Thank you for this opportunity and absolutely if there is any need for any further involvement, I would be happy to do so. Thank you very much Mr. Chairman, Sir and honourable Members.

MR. CHAIRMAN.- Thank you again Sir.

The Committee adjourned at 11.17 a.m.

# **[VERBATIM REPORT]**

## **MEETING OF THE S/C ON FOREIGN AFFAIRS & DEFENCE**

### **CONVENTION**

**Convention on Cybercrime (Budapest Convention)**

**SUBMISSIONS: (1) Mr. Semi Tukana, Sole Limited.  
(2) Pacific Islands Forum Secretariat  
(PIFS)**

**VENUE: Big Committee Room (East Wing)**

**DATE: Thursday, 13<sup>th</sup> April, 2023**

**VERBATIM REPORT OF THE MEETING OF THE STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE HELD IN THE COMMITTEE ROOM (EAST WING), PARLIAMENT PRECINCTS, GOVERNMENT BUILDINGS, ON THURSDAY, 13<sup>TH</sup> APRIL, 2023 AT 8.57 A.M.**

**Interviewee/Submittee:** Sole Limited

In Attendance:

Mr. Semi Tukana - Founder of Software Factory - Sole Limited

-----

MR. CHAIRMAN.- Honourable Members, members of the public, the Secretariat and ladies and gentlemen; a very good morning to you all and it is a pleasure to welcome everyone, especially the viewers who are watching this proceeding.

This is a meeting of the Standing Committee on Foreign Affairs and Defence and for your information, pursuant to Standing Order 111 of the Standing Orders of Parliament, all Committee meetings are to be open to the public. Therefore, please, note that this submission is open to the public and media and is also being streamed live on the Parliament website and social media online and the Parliament Channel on the Walesi platform.

For any sensitive information concerning the matter before us this morning that cannot be disclosed in public, this can be provided to the Committee either in private or in writing. Please, be advised that pursuant to Standing Order 111(2), there are only a few specific circumstances that allow for non-disclosure and these include:

1. National Security matters;
2. Third party confidential information;
3. Personnel or human resources matters; and
4. Committee deliberation and development of Committee's recommendation and report.

I wish to remind honourable Members and our guests that all questions are to be addressed through the Chairman. This is a parliamentary meeting and all information gathered is covered under the Parliamentary Powers and Privileges Act. Please, bear in mind that we do not condone slander or libel of any sort and any information brought before this Committee should be based on facts.

In terms of the protocol of this Committee meeting, please, minimise the usage of mobile phones and all mobile phones to be on silent mode while the meeting is in progress.

(Introduction of Members of the Standing Committee)

Today, the Committee will be hearing a submission on the Convention on Cybercrime, otherwise known as the Budapest Convention. For the purpose of the viewers who are joining us this morning, allow me to give a brief explanation on the Treaty.

The Convention on Cybercrime, also known as the Budapest Convention, provides a comprehensive and coherent framework on cybercrime offences and electronic evidence. It serves as a guideline for any State that is developing a comprehensive national legislation against cybercrime and as a framework for international cooperation amongst States Parties. To- date, the Convention has 67 member States which includes Australia and Tonga from the South Pacific region.

Pursuant to Article 37 of the Convention, any other State, such as Fiji, can become a Party by accession, if the State is prepared to implement the provisions of the Convention and upon invitation to accede to the Convention after consultation and approval of Parties. With the extreme effects of global cyber threats and attacks on critical sectors such as finance, ICT, energy, water, emergency services, public safety, health, public services, aviation and e-government infrastructure, becoming a Party to the Convention will enhance Fiji's ability to combat cybercrime, with international support and assistance particularly in relation to continued capacity building, to better equip Fiji's criminal justice authorities, including the judiciary, prosecution and law enforcement agencies.

Ladies and Gentlemen, before us this morning we have Mr. Semi Tukana, the founder of Software Factory Limited and Sole Limited and I request Mr. Tukana to introduce himself and to begin his submission, after which there will be a question-and-answer session. *Vinaka Vakalevu*, Mr. Tukana, the floor is yours.

MR. S. TUKANA.- The Chairman of the Parliamentary Standing Committee on Foreign Affairs and Defence, especially the Convention on cyber security, and to the honourable Members of the Committee, thank you so much for the invitation you have given me to come this morning and to present our submission to this esteemed Committee.

First of all, by way of introduction, my name is Semi Tukana, I am from Vanuavatu, a small island in the Lau Group and *vasu* Muamua in the *Tikina* of Mualevu in Vanuabalavu. I am married for 37 years with four adult children and four grandchildren.

By way of academia, I went to Marist Brother High School and then to USP. I did my Bachelor of Science in Physics and Mathematics, entered into the workforce in IT, then did my Postgraduate Diploma in Computer Science at the Queensland University of Technology. I went across to the University of Queensland and did my Masters.

I have been in the industry for 41 years. I am 62 years old now, still going on just like you, and I am glad I can see honourable Naivalurua here. We were together at Marist, and we are still going.

My role in the IT industry is to design systems and keep the information of our people. For 41 years I have been developing systems, designing systems and implementing systems in corporate organisations until two years ago when we started doing Sole. Now, we have moved into the public arena - it is public access. It is no longer something that is confined to an organization, like for a bank, where we go and implement a system, it is a private network with private membership. Now, no more.

With Sole, everyone can come on board from anywhere in the world. So, we are acceptable to cyber-attacks now, and that is the reason I take my coming this morning seriously, Mr. Chairman and honourable Members of the Committee, and the words that have been provided in this submission is given in all seriousness.

You may see also that I have a contributor to the submission, his name is Bob Adhar. By way of introduction, he is actually from Vuci in Nausori. We did Foundation studies together at USP and he then went on a scholarship to South Australia and Adelaide and never came back. But thank God, he stayed because he then formed a company for cyber security. So, now, we have joined forces and that was about 15 years ago. Everywhere I go I develop a system, implement it, I call in Bob, "Come and do a penetration test on this system. Make sure that it is solid." That is how our friendship is formed.

People look to me as though I am the cyber security expert in Fiji - it is a disclaimer, I am not a cyber security expert. I am a systems designer and a systems developer. There are people who are experts in this field and Mr. Bob Adhar is the expert in cyber security. So, most of the presentation this morning, we had discussed, and he said, "Alright, let us put this together for the benefit of the community and also for the nation."

On the macro view, Fiji is in the process to ratify the Budapest Convention on Cybercrime and in the process of legislating the Cyber Crime Act 2021, the Constitution of the Republic of Fiji provides for a right to privacy, but we believe it lacks specific personal data protection legislation. The general data protection regulations set the standard similar legislation now being passed and enforced worldwide, mandating the use of encryption to protect our citizens data and also the effective encryption is now essential for protecting citizens data and maintaining economic health.

On a micro view, we believe that Fiji should create its own privacy standards and be enforced immediately. I am speaking from a practicing systems designer and I need protection around the systems that I deal with, especially now that we have moved into the digital financial banking and trading platform.

We are saying that it might be easier for us to benchmark against the Australian data privacy standard and other similar standards that they have adopted, and we can customize it for Fiji's case. The standard should be mandatory to be implemented by all businesses and Government Departments in Fiji. We have had two recent attacks in two of the organisations that I am closely involved with, these are ransomware. We are very lucky that the two organisations are still operating.

It is coming close to home now so now is the time for us to fast-track this particular case – the cybersecurity space. Before, I used to have a *laissez-faire* – a no-care attitude - I just design the systems and no one can penetrate these systems. It is no more. No! It is so complex now that there are cyber-attacks happening almost as we speak.

There should be fines, yes. If we do not enforce this legislation through some penalties, then our organisations will treat it very lightly, so there has to be some kind of penalties involved here. Speaking from a company that does this, that means that I too have to pay fines if I do not comply.

You have read the submission, the cyber measures to protect data. We look at personal data at the personal data level, at the corporate data level and that at the national level. That is the way I look at things. We have to have legislation to protect a person's data, the privacy and the identity of the person.

We have to put legislation to safeguard organisations because they have thousands of people who are using that system for the corporation and then we have to have legislation to protect us at the national level and I think that is the way we should be looking at this.

So, I have put down there firewall (of course, firewall has been there for 30 years or 35 years, or something like that), antivirus malware, access controls, network monitoring and security policies. It is important that we now need to enforce that corporations need to have cybersecurity policies in place for our organisations, and not only the banks. My role is developing banking systems, so not only banks but all organisations, including our hospitals. All systems must have a cybersecurity policy. Then, of course, we have physical security and then we go down to the level of data encryption.

We are saying here that we need to recommend going harder on encryption. The reason is this – if a force has managed to break down our security doors, they come in and break down the safe, they have the documents right in front of them. They can read it, and if it is not encrypted, that is it. All the data can be sold, or they can be used in a malicious way outside, so that is why we are saying that encryption is our final line of defence and we need to take that seriously.

There are some data fields in databases but not all, that are so critical that we need to encrypt those data because we must think like this – if we have all the databases encrypted and the processing power needs to decrypt and then process, it is going to be expensive. We need critical data fields that are needed to be protected and encrypted. We need to weigh the two - encrypt the whole database, we need super computers to encrypt, process and encrypt again. That is the reason why we are saying now that we need to really look at ways in which we could legislate the need to put in place encryption policies and regulations for all key strategic organisations that cater for people.

We have there - when other cybersecurity measures fail, as I had mentioned before, it is encryption which is our last bastion of defence.

Have higher level of encryption like folder and field level encryption, separate storage and management for keys and data - these are cybersecurity terms where keys are stored separately to decrypt, and that needs some specialized management and specialist care for those keys.

Role separation – of course, protect data from IT administrations. Now, we need to protect data even from our own people inside. It is a bit hard but if you have proper segregation of duties in certain areas of IT, then we should be able to protect data. I think if we do this in Fiji, we are going to rise to another level. At the moment Fiji is an open field - welcome to Fiji. That is basically where we are at the moment. In here, we are trying to move to another level and cybersecurity attacks are now prevalent, so we put in place this legislation to protect us. Minimum access rights, even tighter encryption in place.

Example of fines are here and some are saying GDPR fine of four percent of annual revenue, this is what we are saying, coming from the European example, some are even fined for €20 million. Perhaps, we can custom-made for Fiji, may be not too hard as we start, then give a timeframe and then we say, “Listen, no more, we need to enforce this”, the level of fines that we need to have.

So, we are looking at emails, our credit card data, health record, et cetera. My company develops our hospital systems, -banking systems, provident fund systems. As you are born, you would be involved with our company - from when you are born, when you go and lease a land from iTLTB, we will take care of you. When you borrow money, we will take care of you, even when you die and you do not leave a will, our system will take care of your estates. That is the systems that we build. When you go to university, our systems will take care of your grades and everything that happens at university level. That is where the experience comes in, in that we are exposed to cyberattacks now and we will need to put in place these legislation or regulations or policies to protect our data.

Coming from someone who has built a horizontal level of wall systems in Fiji and the Pacific, I am hoping that we could set the benchmark here in Fiji and I am sure that all the other Pacific Islands are going to follow suit. So, as we build systems and we implement it throughout the Pacific, it is important for us to set the benchmark on cybersecurity and also trickle it down to all the other Pacific Islands.

I have some diagrams there which is self-explanatory - the data protecting our system. So, data is in a storage medium, and it needs to be protected. When the data is transmitted (this line), it needs to be protected. Then at the user end, there needs to be protection, so when we are talking about cybersecurity, we need to protect this level of storage, the transmission and the user access on the other side. That is when we are coming down to corporate level, to personal level and hopefully, we will rise up to the national level - we will put a cyber security bubble, as we say, just to cover the whole nation of Fiji.

Once we protect that, we cannot say that we are completely safe - we need to be vigilant, but we can say, "to some extent, we are protecting our data". I have to give some kind of comfort to our users. People are asking, how safe is Sole? People from America and the United Kingdom have set up their accounts in Sole. How safe is Sole? I am going to save my money there. Then I have to say, "Listen, we have done penetration test on the outside, they could not get in."

Our partners in cybersecurity had to ask for us to open the door for them to come into the system and for them to attack from within. They found some vulnerabilities inside. I say this in public, I have already mentioned it, but they provide the fix for it. So, we have fixed those holes inside and then we asked them again, "Now, come back in again. Come inside the door and try to hack the system", but they could not. And we have to repeat it every six months. So, this is not a once the hole is plucked, everything is safe, no! We cannot say we will be 100 percent safe from outside the bank. This is going to continue.

Protection of Application - I have already mentioned this about databases and cloud virtual machines. On containers, again, encryption, access control and we have to look at blacklisting and whitelisting. Now, we need a scrubbing system that will only allow whitelisted IP addresses of countries that are safe. We need to do scrubbing before things come into the country. I am glad I met someone yesterday, a local as well, who are about to introduce this. It will be good for us as a nation to have this scrubbing of access before they come into the country.

Audit trail is very important of every file access events. Every time someone inquires in the database or come into a network, we need to have audit trails for that. Of course, we need to have centralised management for our protection.

Coming to my two last pages of presentation, I am looking here at our sovereign core data and systems infrastructure. This is very close to my heart. I must declare that I have vested interest in this, but I am not ashamed to mention it in public that we need to get back our core data and systems infrastructure back into the nation. These are systems that are core to the proper functioning of our organisations and of our nation of Fiji. These systems must protect our people. Some people say, "Oh, systems will not affect our lives." No, people live and people die when systems are not running efficiently, effectively, and if it is totally attacked, people die of stress. So, this is a matter of life and death. I tell people, "If we do a proper system, people will be happy."

So, these systems are important for the prosperity of this nation. It must be designed and developed by core of local systems designers and developers. We have the competency here in this country to do this and we do not need to go abroad to outsource all these systems, no need. I can prove that because I replaced the number one ERP solution in the world - ACP at the iTaukei Land Trust Board to 2009.

That is the number one ERP solution in the world. We spent a lot of money on it - four years, 25 foreign consultants, they nearly brought that place done. Until they re-tendered, we won, we developed it - 10 months, four months to design, six months to develop with only six of us and three of those were fresh graduates from the University of the South Pacific (USP).

We have the capabilities to design and to develop our own systems. We are a small nation. We must never think we are big. No, we are a small nation, and it is easy to manage things when we are small. It is not complex. We must always bear that in mind.

The data also must be domiciled here in Fiji. Source codes - whatever critical systems that need to be developed, the source codes must reside here in Fiji. They must not go and say, "We will develop over there, implement it there, you run it." No, you will be at their mercy, and we have the problem right now in a couple of organisations. I am saying, at the national level, we need to somehow protect this.

Foreign systems developers, I must say, we can call in specialists to come in and join when we are developing systems that are critical for the nation - call in specific expertise, and we do need those from time to time.

What other systems that I believe are critical core data systems infrastructure in this nation? I am looking at our Election Information Management System, I am looking at our Immigration Management System, these can all be developed in this country. The Birth, Death and Marriages System can be developed in this country, domicile the data in the country and ensure that we have source codes in the country.

Passport Management System, the Judicial Management System, Police Intelligence and Law Enforcement Management Systems, Military Defence and Homeland Security System, Hospital Information System, Registrar of Companies Management System, Registrar of Titles and, of course, our Integrated Tax Management System, nothing compliance. We can develop all these systems here in Fiji using our own people, domicile the data here and ensure that our source codes are here in Fiji.

Mr. Chairman and honourable Members of this Standing Committee on Foreign Affairs and Defence, especially on the area of the Budapest Convention on Cybercrime, thank you very much.

MR. CHAIRMAN.- Thank you, Mr. Tukana, for that very enlightening and comprehensive presentation, putting into perspective some of the requirements that we will need to put in place, given that today we are talking about signing up to a Convention at the strategic level and the implications of what we should be doing, so I thank you so much for your presentation today. It is an honour to listen to you this morning.

Honourable Member, the floor is now open for any questions.

HON. L.S. QEREQERETABUA.- Mr. Chairman, if I may, through you, thank you very much, Mr. Tukana. Absolutely enlightening, *vinaka sara vakalevu*.

I thank you, especially for those last two slides, highlighting the fact that a lot of our data is domiciled overseas and also the source codes. I remember honourable Tikoduadua talking about the immigration data, I think, one of the systems that needs to be updated, we need to pay an arm and a leg to have the administrators come in and fix the problem here. In terms of the Budapest Convention (Convention on Cybercrime), what is your own personal and professional opinion on whether or not Fiji should ratify?

MR. S. TUKANA.- Thank you, honourable Member, and Deputy Speaker. I think we have mentioned here that we really need to ratify the Convention. We just need to ensure that in our case, it is customized for our country. It will take time for people to comply, and we need to think of the practicalities on the ground. If we do not, then there is going to be some flacks from major corporations in trying to comply, but it can become very expensive. As long as we are given time to comply, but ratifying the Budapest Convention, we are all for it.

HON. L.S. QEREQERETABUA.- Just a follow up question, Mr. Chairman; when you said 'time to comply', how much time will we be looking at?

MR. S. TUKANA.- Five years.

HON. I. NAIVALURUA.- Mr. Chairman, through you, I congratulate Mr. Tukana for your achievements and your very educational and enlightening presentation this morning. I noted that in your presentation, it said that Fiji is an open field. I just wanted to know when we compare where we are today to other developed nations, how would you grade our position and where are we?

MR. S. TUKANA.- Maybe, four out of ten, yes, that low. We are an open field, and we should move up to about seven or eight out of ten by having cyber security policies in place and people will be more serious about it. There is a laissez-faire kind of attitude in organizations, mine included. It was only when I started introducing the new platform 'the Sole' that I become really serious about cyber security.

Prior to that, when we implement systems in organisations, we think that the firewalls will protect us, no, no more. So we are an open field right now and there are people and organisations out there. In my 41 years in IT and I still have a 'no care' attitude on cyber security until we started moving into that public digital space, then it dawned on me that this is much more serious than we thought. Before, it was ensuring the processing is done correctly, the interest calculation is to the cent, but now it is a little bit more complex than that.

HON. I. NAIVALURUA.- Mr. Chairman, just a follow up question; how would you assess the understanding of cyber-crime in the community at large from the private sector and public sectors, is it being advocated

properly in the schools? Do we know what is the major threat ahead of us? I really wanted to hear your thoughts on that.

MR. S. TUKANA.- Mr. Chairman, thank you. It is only at university level that they have introduced some subjects on cyber security. At USP, we now have a security network engineering course which is accredited to the Australian Computer Society. We have a software engineering course and we have network and security. It is this network and security that have now some component on cyber-security but as far as going down to the secondary or high school level, (if I am not mistaken) it is zero at the moment.

I sit on the USP Council and I know that is the reason why we have some level of cyber security course, but it needs to be made like a course on its own, like a full Bachelor of Science in Cyber Security rather than Bachelor of Networks and Security, where it is just one or two units on cyber security. I think we need to move up to the space list level, so to answer your question, it is very low.

I am talking for myself, for 41 years and I still have very low understanding on the problem because these things keep on changing. You thought you have mastered it and cyber attackers have gone into another level. You move there and they move to another level. That is the reason why I believe that we need to have a specialist undergraduate course specifically for cyber security.

MR. CHAIRMAN.- We may have one more question.

HON. J. VOCEA.- Mr. Chairman, through you, now that we have a Cyber Security Act in Fiji, just listening to your presentation and the vulnerabilities that our systems have now, the data and all that, do you think or feel that we still need to develop some more policies to protect our systems both, in the private and the public sectors?

MR. S. TUKANA.- Thank you, Mr. Chairman, to be honest, I have not read the Cyber Security Act 2021. I will need to take time to read that and provide a formal response to the Standing Committee on that particular question.

MR. CHAIRMAN.- *Vinaka vakalevu*, Mr. Tukana. We would love to have that from you on your views on that Act also.

If I may, on behalf of the Committee, Mr. Tukana, I would like to thank you sincerely for coming in this morning to talk to us. Secondly, for me, I am going to go back and read the verbatim reports of discussions on this Cyber Security Convention. There is a lot of things that you have said are very relevant to what we are discussing, as far as signing up to the Convention.

We are also looking at the end result of signing up to the Convention, as we had talked about it today on what we need to put in place because sometimes, we sign up to Conventions and leave it there. I was thinking about monitoring the implementation, what is required and you have really shed some light into what we should be looking out for when we sign up to the Convention.

On behalf of the Committee, Mr. Tukana, *vinaka vakalevu* and thank you so much. Thank you for the work that you do, and we wish you well. We hope that you will make yourself available should we still need to talk to you further on this.

MR. S. TUKANA.- *Vinaka*, Mr. Chairman. Once again, thank you, honourable Members of the Standing Committee on Foreign Affairs and Defence, for inviting me.

MR. CHAIRMAN.- I will now adjourn the meeting.

The Committee adjourned at 10.09 a.m.

**Interviewee/Submittee:** Pacific Islands Forum Secretariat (PIFS)

In Attendance:

1. Mr. Paki Ormsby - Director Policy
  2. Mr. Michael Crowe - Regional Security Advisor
  3. Mr. Jonetani Tagivetaua - Political Governance Advisor
- 

MR. CHAIRMAN.- Honourable Members, I call the meeting to order.

Honourable Members and members of the public, the Secretariat, ladies and gentlemen; a very good morning, again, to all of you. It is a pleasure to welcome everyone this morning, especially the viewers who are watching this proceedings.

This is a meeting of the Standing Committee on Foreign Affairs and Defence. For your information, pursuant to Standing Order 111 of the Standing Orders of Parliament, all Committee meetings are to be open to the public. Therefore, please, note that this submission is open to the public and the media, and is also being streamed live on the Parliament website and social media online platform and the Parliament Channel on the Walesi platform.

For any sensitive information concerning the matter before us this morning that cannot be disclosed in public, this can be provided to the Committee either in private or in writing. Please, be advised that pursuant to Standing Order 111(2), there are only a few specific circumstances that allow for non-disclosure, and these include:

1. National Security matters;
2. Third party confidential information;
3. Personnel or human resources matters; and
4. Committee deliberation and development of Committee's recommendation and report.

I wish to remind honourable Members and our guests that all questions to be addressed through the Chairman. This is a parliamentary meeting and all information gathered is covered under the Parliamentary Powers and Privileges Act. Please, bear in mind that we do not condone slander or libel of any sort and any information brought before this Committee should be based on facts.

In terms of the protocol of this Committee meeting, please, minimise the usage of mobile phones and all mobile phones are to be on silent mode while the meeting is in progress.

Allow me to introduce the Members of the Committee.

(Introduction of Members of the Standing Committee)

Today, the Committee will be hearing a submission on the Convention on Cybercrime, otherwise known as the Budapest Convention. For the purpose of the viewers who are joining us this morning, allow me to give a brief explanation on the Treaty.

The Convention on Cybercrime, also known as the Budapest Convention, provides a comprehensive and coherent framework on cybercrime offences and electronic evidence. It serves as a guideline for any State that is developing a comprehensive national legislation against cybercrime and as a framework for international cooperation amongst States Parties. To-date, the Convention has 67 member States which includes Australia and Tonga from the South Pacific region.

Pursuant to Article 37 of the Convention, any other State, such as Fiji, can become a Party by accession, if the State is prepared to implement the provisions of the Convention and upon invitation to accede to the Convention after consultation and approval of Parties. With the extreme effects of global cyber threats and attacks on critical sectors such as finance, ICT, energy, water, emergency services, public safety, health, public services, aviation and e-government infrastructure, becoming a Party to the Convention will enhance Fiji's ability to combat cybercrime, with international support and assistance particularly in relation to continued capacity building, to better equip Fiji's criminal justice authorities, including the judiciary, prosecution and law enforcement agencies.

Honourable Members, ladies and gentlemen; before us this morning, we have the team from the Pacific Islands Forum Secretariat. I request Mr. Ormsby to introduce his team and to begin his submission, after which there will be a question-and-answer session. Thank you, Mr. Ormsby, the floor is yours.

MR. P. ORMSBY.- Thank you, Mr. Chairman, for this invitation and to the honourable Members of the Committee, a warm greetings this morning.

On behalf of the Secretary-General, it is a privilege to be here to present our submission today. On behalf of our colleague, Mr. Terio Koronawa, who is sick and sends his apologies that he is not able to be here with me today, it falls on my shoulders to present the submission, otherwise Mr. Koronawa would be here.

However, before I do that, Mr. Chairman, let me just offer the opportunity to my colleagues, who will be very familiar to you all, to introduce themselves to you and then I will proceed with my submission. Thank you.

(Introduction of PIFS Officials)

MR. P. ORMSBY.- Mr. Chairman, my colleagues are here to take all the hard questions so any of those are to be directed to my left.

Mr. Chairman, the Pacific Islands Forum (PIF) is the region's premier political and economic policy organisation. Founded in 1971, it now comprises 18 members including Australia, Cook Islands, Federated States of

Micronesia, Fiji, French Polynesia, Kiribati, Nauru, New Caledonia, New Zealand or Aotearoa, Niue, Palau, Papua New Guinea, Republic of Marshall Islands, Samoa, Solomon Islands, Tonga, Tuvalu and Vanuatu.

The Forum's Pacific Vision is for a regional peace, harmony, security, social inclusion and prosperity, so that all Pacific people can lead free, healthy, and productive lives. The PIF works to achieve this Vision by fostering cooperation between governments, collaboration with international agencies and by representing the interests of our members both regionally and globally.

In July 2022, our PIF Leaders endorsed the 2050 Strategy for the Blue Pacific Continent. The 2050 Strategy sets out the region's approach to collectively work together to achieve the long-term vision and aspirations for our region through seven key thematic areas.

In terms of our discussion today on cybercrime, two of those seven key thematic areas are directly relevant - the Thematic Area on Peace and Security and the Thematic Area on Technology and Connectivity.

Mr. Chairman, we have provided copies of the 2050 Strategy for four members, alongside our original Security Report for your consideration.

In terms of regional security policy, the vision outlined in the 2050 Strategy builds on and reaffirms Forum Leaders' 2018 *Boe Declaration on Regional Security*.

In the 2050 Strategy, Leaders reiterated the expanded concept of security for our Pacific that had been identified in 2018, that includes cybersecurity and a shared vision that all Pacific peoples benefit from their access to affordable, safe and reliable land, air and sea transport and ICT infrastructure, and systems and operations, while ensuring culturally sensitive user-protection and cyber-security.

Mr. Chairman, linked to the 2050 Strategy and the 2018 Boe Declaration on regional security, Forum Leaders outlined an expanded concept of security for our Pacific region. Recognising that among other challenges, cybercrime posed an increasing threat to the safety and wellbeing of the peoples of our Blue Pacific Continent and Leaders reaffirmed that cybersecurity was a priority security challenge but required a collective regional effort to address.

The Forum Secretariat continues to assess that cyber security issues, specifically cybercrime and cyber-enabled crimes, will continue to negatively impact the peace and prosperity of Pacific peoples, and that continued effort is required by all of our members and partners to mitigate this threat.

Mr. Chairman, following the *Boe Declaration on Regional Security* in 2019, Forum Leaders endorsed the Boe Declaration Action Plan, which outlines a range of proposed actions to combat security threats, including a full strategic focus area on cyber threats.

Mr. Chairman, to address cybercrime, Forum Members committed to five key actions:

1. Sharing information on cybersecurity and cybercrime threats through relevant fora such as the Pacific Cybersecurity Officials Network.
2. Supporting the development of national cyber policies/strategies and legislation.
3. Promoting awareness and educating our people on responsible cyber behaviour.
4. Developing and strengthening our computer emergency response teams.
5. Promoting and supporting Forum Members' accession to the Budapest Convention on Cybercrime.

Mr. Chairman, before I talk further on the Budapest Convention, I wish to highlight an underlying premise of regional security recognised by our Forum Leaders in the *Boe Declaration on Regional Security*, that national security and each and every one of our foreign member countries, impacts on the security of the region as a whole.

Noting this premise, Forum Members have committed to strengthening respective national security approaches, and thus contribute to security of the whole Blue Pacific Continent.

In terms of cybersecurity, Forum Members have done this in a number of ways, in line with the Boe Declaration Action Plan:

- Tonga, Samoa, Kiribati, Vanuatu and Papua New Guinea (to name just a few) have developed national computer emergency response teams.
- Several Members have worked closely with the Pacific Islands Chiefs of Police Network to enhance cyber-safety awareness with online-hygiene programmes in schools and workplaces.
- Vanuatu and Kiribati have developed national cyber security strategies, and all Forum Members, including Fiji, are sharing information on cybersecurity, through the Pacific Cybersecurity Officials Network and the Pacific Transnational Crime Network.
- Directly related to today's discussion, several Members have significantly progressed their efforts to accede to the Budapest Convention on Cybercrime.

The Budapest Convention on Cybercrime is regarded by Forum Members as the most comprehensive and coherent international agreement on cybercrime and electronic evidence to-date. It serves as a guideline for any country developing domestic legislation on cybercrime and as a framework for international cooperation between State Parties to the Convention.

The Budapest Convention provides for:

1. the criminalisation of conduct, ranging from illegal access, data and systems interference to computer-related fraud and child pornography;

2. procedural powers to investigate cybercrimes and secure electronic evidence in relation to any crime; and
3. efficient international co-operation - the Treaty is open for accession by any country.

In terms of Pacific Islands Forum Members, Australia and Tonga have already acceded to the Budapest Convention. Like Fiji, Vanuatu and New Zealand have been invited to accede by the current Parties to the Convention, after indicating their interest in accession. This invite shows that these countries have drafted laws that indicate they have implemented or are likely to implement the provisions of the Budapest Convention in their domestic law.

It is our view at the Forum Secretariat that Fiji's accession to the Budapest Convention would provide further momentum and inspiration for fellow Forum Members to continue their own national efforts to accede. We believe that acceding to the Convention is not just in Fiji's interest, but by extension, it is in the region's interest also, and supports regional efforts as outlined under the Boe Declaration and the 2050 strategy.

We want the region to become a hard target for cybercriminals. We did not want to be a soft target. We want cybercriminals to know that if they perpetrate cyber-related fraud, crime, interference, forgery and trespassing anywhere in the Blue Pacific Continent's cyber domain, including here in Fiji, they can and will be caught, tried and prosecuted.

In concluding, we wish to highlight that the Forum Secretariat is aware of a range of support that is available to Forum Members to aid their efforts to accede to the Budapest Convention, and we want to underscore that Fiji is not alone in its efforts to accede and any support can be provided from the Forum Secretariat.

The Pacific Islands Legal Officers Network hosts a Cybercrime Working Group, which brings Forum Members together to exchange information and lessons learned, including on Budapest Convention accession efforts. That network has a close working relationship with the Council of Europe (the host of the Budapest Convention) and facilitates assistance between the Council of Europe's development assistance programme, known as the Global Action on Cybercrime Plus (GLACY+) and Forum Members, as well as other developing nations the world over.

The purpose of that programme is to strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence to enhance their abilities for effective international cooperation in this area. We understand Fiji has engaged with this programme in the past and we have received indications from the Council of Europe that it intends to continue to support Forum Members, including Fiji, with such efforts into the future.

Further, just as we do for all our Members on a broad range of security issues, the PIFS, your regional Secretariat, remains ready to assist in any way we can to support Fiji in its national security development efforts. This includes on cybersecurity, as well as the support in relation to your accession to the Budapest Convention.

I wish to highlight recent comments from Fiji's neighbour and fellow our Forum Member, Tonga, who has also acceded to the Budapest Convention.

While acknowledging that more work is still required to fully realise the benefits of accession to the Budapest Convention, the Attorney-General of Tonga recently presented to fellow Forum Members that Tonga's accession to the Budapest Convention has afforded it with an opportunity to align its domestic laws with that of 67 other countries worldwide who are leading the fight against cybercrime. By having laws that are better aligned with those 67 countries, Tonga has a sound basis on which to build interoperability in dealing with the transnational nature of cybercrime.

Until the whole region has acceded to the Budapest Convention, there will likely remain gaps in our ability to work together to prosecute cybercriminals. Fiji's accession and subsequent efforts will help fill one of those gaps, and thus make our region a little bit more safe and secure.

Thank you, Mr. Chairman for the opportunity to make this humble submission and we thank you for your time today.

MR. CHAIRMAN.- Thank you, Mr. Ormsby, for that presentation from the regional perspective, understanding that cybercrime is a transnational and trans-boundary that we need to deal with it regionally rather than individually. I agree totally with you on plugging the gaps.

I think when countries around us are more secure, it makes the other countries more vulnerable, and we need to be together in trying to build security in cybercrime.

Thank you so much for coming in to make a presentation this morning. I will now open the floor for any questions from honourable Members.

HON. I. NAIVALURUA.- Through you, Mr. Chairman, thank you for your enlightening presentation this morning. In the spirit of Boe Declaration, is there an anticipated timeline where the other Member States would be working towards a more regionalised effort on this particular issue on cybercrime or cybersecurity which brings the convergence of work towards this particular major threat for our part of the world?

MR. M. CROWE.- Mr. Chairman, in terms of the timeline, in short, 'no'. The 2019 Boe Declaration Action Plan which outlines the proposed actions that the region committed to, including accession to the Boe Declaration by each Forum Member country, does not specify timelines and that is because many of our Members are in very different stages and at very different capabilities to undertake the legislative changes required to accede to the Convention. So in many ways, Australia and Tonga have led the way by acceding already, and Vanuatu, New Zealand and Fiji proceed to accede, and we will also be leading the way for the rest of the membership.

At an official level, we received approval from the Boe membership late last year, to enhance or hasten our efforts to support the membership to take further action to accede. So in this year's workplan, the Security

Team within the Forum Secretariat is more actively engaging with Members to bring them together with the Council of Europe, who hosts the Budapest Convention, to understand better where each of our different members are up to in their process of acceding to the Convention, and then applying specific support based on that context for each Member.

MR. CHAIRMAN.- Just a follow on question from that, the Council of Europe, do they have to come through the Forum to us and for us through the Forum to them or we can go directly to them?

MR. M. CROWE.- Mr. Chairman, again in short, 'no', all countries have a direct relationship with the Council of Europe. But, if countries do have to work through the Council of Europe to seek that invitation which Fiji has already been granted from all of the Parties to the Budapest Convention to then be able to accede. So the PIFS just plays a supporting and coordinating role rather than being a central step in the process for, in this instance, Fiji.

MR. CHAIRMAN.- Would you have any ideas as to how far Vanuatu and New Zealand are in, what stage are they in? We are at this stage as far as our accession efforts are concerned. Our next step would be to table this in Parliament. Would you have any idea on how far those two countries are in?

MR. M. CROWE.- Thank you, Mr. Chairman. As mentioned, we are currently working with the Pacific Islands Legal Officers Networks and Cybersecurity Working Group and the Council of Europe to support the undertaking of a mapping exercise to understand where all of the Members are and at what stage the respective Members are up to in their plans to accede to the Budapest Convention.

We do not know yet or at the moment specifically where New Zealand and Vanuatu are up to, but they have certainly been invited to accede to the Convention, which means that as the Director mentioned in his submission, the 67 other existing Parties to the Budapest Convention have accepted that Vanuatu and New Zealand have sufficient progress in drafting domestic legislation and making domestic policy arrangements that indicated they are not far away or they are well advanced in their process of acceding to the Convention.

MR. P. ORMSBY.- Mr. Chairman, if I may, just some supplementary comments to my colleague's response, we have a meeting next Tuesday - the Forum Sub-Committee on Regional Security. At that meeting, we will seek an update from New Zealand and Vanuatu on their progress and provide that information back to the Sub-Committee.

I also have some supplementary background notes on the Council of Europe, as well as the cybercrime update from the Regional Security Outlook Report that we have provided to your Committee as well, which outlines the two-year projection for cybercrime across our region.

We do note, following regional meetings in Singapore last year, that the global comments in what we call, the webspace, is only 23 percent controlled by government. So, that is an important point to recognise when we are looking at the global comments of the digital global space because we will need the close support and alignment of the private sector and the civil society as well to align into the global cyber behaviour.

Financial institutions are key in that, as we know all of our banking is cyber, it is online banking now, and we are moving to there, and how we regulate a lot of that.

I guess the point that I am trying to make is that accession to the Budapest Convention provides you with the framework to start that process of looking to better regulate and normalise behaviours online. As we know, a lot of our regions, through social media and even through this Committee meeting today, we are connecting closely to our people and we need ways to keep them safe when online as we do that, and this work helps to enhance and protect them from cybercrime.

MR. CHAIRMAN.- Thank you. If there are no further questions, on behalf of the Committee, I thank the Team from the PIFS for coming in and presenting to us. Thank you for sending us this brief earlier. We had an opportunity to read through this morning. I hope that you will be available should we wish to clarify some issues further and we would love to have that result of the SubCommittee meeting on Tuesday and if you can provide that to us as well.

Again, I thank you for taking your time to come in and talk to us. I wish Mr. Koronawa speedy recovery. Tell him to drink a lot of water. Again, on behalf of the Committee, *vinaka vakalevu*, and to the honourable Members, I will declare this meeting closed.

The Committee adjourned at 10.09 a.m.

# **[VERBATIM REPORT]**

## **MEETING OF THE** **S/C ON FOREIGN AFFAIRS & DEFENCE**

### **CONVENTION**

**Convention on Cybercrime (Budapest Convention)**

**INSTITUTION: Online Safety Commission Fiji**

**VENUE: Big Committee Room (East Wing)**

**DATE: Thursday, 27<sup>th</sup> April, 2023**

**VERBATIM REPORT OF THE MEETING OF THE STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE HELD IN THE BIG COMMITTEE ROOM (EAST WING), PARLIAMENT PRECINCTS, GOVERNMENT BUILDINGS, ON THURSDAY, 27<sup>TH</sup> APRIL, 2023 AT 8.57 A.M.**

**Interviewee/Submittee:** Online Safety Commission Fiji

In Attendance:

1. Ms. Tajeshwari Devi - Acting Commissioner
2. Mr. Savenaca Siwatibau Waga - Member of Working Group

MR. CHAIRMAN.- Honourable Members, members of the public, the Secretariat, viewers who are watching us live, ladies and gentlemen; a very good morning to you all. It is a pleasure to welcome everyone, especially our viewers who are watching this proceeding.

At the outset, for information purposes, pursuant to Standing Order 111 of the Standing Orders of Parliament, all Committee meetings are to be open to the public. Therefore, this meeting is open to the public and media, and is also being streamed live on the Parliament *Facebook* page and Parliament Channel on the *Walesi* platform.

However, for any sensitive information concerning this submission that cannot be disclosed in public, this can be provided to the Committee either in private or in writing. This can only be allowed in a few specific circumstances which include:

1. National Security matters;
2. Third party confidential information;
3. Personnel or human resources matters; and
4. Committee deliberation and development of Committee's recommendation and report.

I wish to remind honourable Members and our invited submitters that all comments and questions are to be addressed through the Chairman. Also be mindful that only the invited submitters will be allowed to ask any questions or give comments to the Committee. This is a parliamentary meeting and all information gathered is covered under the Parliamentary Powers and Privileges Act and the Standing Orders of Parliament.

In terms of the protocol of this Committee meeting, please, be advised that the movement within the meeting room will be restricted. Please, minimise the usage of mobile phones and all mobile phones are to be on silent mode while the meeting is in progress.

(Introduction of Members of the Standing Committee)

With us this morning, we have representatives of the Online Safety Commission (OSC), who had been requested to provide a submission on the Convention on Cybercrime. For the purpose of the viewers who are joining us this morning, allow me to give a brief explanation on the Treaty.

The Convention on Cybercrime, also known as the Budapest Convention, provides a comprehensive and coherent framework on cybercrime offences and electronic evidence. It serves as a guideline for any State developing a comprehensive national legislation against cybercrime and as a framework for international cooperation amongst State Parties. To-date, the Convention has 67 Member States which includes Australia and Tonga from the South Pacific region.

Pursuant to Article 37 of the Convention, any other State, such as Fiji, can become a Party by accession, if the State is prepared to implement the provisions of the Convention and upon invitation to accede to the Convention after consultation and approval of the Parties.

With the extreme effects of global cyber threats and attacks on critical sectors such as finance, ICT, energy, water, emergency services, public safety, health, public service, aviation and e-government infrastructure, becoming a Party to the Convention will enhance Fiji's ability to combat cybercrime, with international support and assistance particularly in relation to continuous capacity building to better equip Fiji's criminal justice authorities, including the judiciary, prosecution and law enforcement agencies.

I take this time to invite our submitters to introduce themselves before we proceed with the submission. Please, note that if there are any questions by honourable Members of the Committee, they may interject or we will wait until the end of your submission to ask our questions.

You may now introduce yourselves and then make your submission. Thank you.

MS. T. DEVI.- Good morning, Mr. Chairman and honourable Members of the Standing Committee. It is a privilege and honour to be here this morning. I would like to show appreciation to the Standing Committee for inviting the Online Safety Commission (OSC) to provide views on the Convention on Cybercrime, whether Fiji should ratify the Convention with or without reservations.

I am Tajeshwari Devi, the Acting Online Safety Commissioner and I am accompanied by Mr. Savenaca Siwatibau Waqa, an active supporting member of the Online Safety Commission's Working Group.

As I may, the OSC empowers Fijians to be responsible and safe online. It provides Fijians a space to resolve concerns with respect to online abuse such as online bullying, internet trolling or imagebased abuse.

The OSC provides an avenue to assist individuals confronted with harmful online content by delivering services and resources that help to minimise the harm and educate ways to be proactive and safe online. These include;

- developing and designing educational content of online safety;
- organising awareness programmes;
- receive and manage online abuse reports from individuals;
- provide access and advice in relation to queries submitted to the Commission;
- investigate online abuse reports through alternate dispute resolution mechanisms that would bring about efficient and reasonable means of redress; and
- collaborate with relevant agencies and Governments to provide the best possible outcome.

We understand that the Convention provides a framework for protecting individual rights in the context of cybercrime investigations and prosecutions. It requires signatories to respect fundamental rights, such as privacy, freedom of expression, and ensures that any measures taken to combat cybercrime are necessary, proportionate and subject to judicial review.

While we commend the State for having national legislation such as the Online Safety Act, the recent Cybercrime Act and Crimes Act that identify computer and cyber-related crimes being a part of this Convention will also require some amendments to those established instruments in order for the Convention to work in unity with established mechanisms.

Since establishment, the OSC has witnessed the rise of online abuse as it relates between persons primarily, such as cyberbullying, image-based abuse, doxing and more. In light of these reports, it is clear that women and girls are disproportionately targeted and abused through online platforms and tools, making them more susceptible to gender-based online violence.

On 14<sup>th</sup> January, 2020, the OSC signed a Memorandum of Understanding with the Fiji Police Force to assist in these specific forms of abuse and other related online abuses, creating effective cooperation that is built on mutual trust, shared non-privileged information and investigating online abuse reports, and seek to resolve those reports in a manner outlined by the Online Safety Act 2018.

This Budapest Convention serves to be an instrument that would allow such cooperation at a higher level. In light of this, it is important to remember the safety of individuals rather than only focusing on the infrastructure or policies alone.

With the effects of global cyber threats and attacks on critical sectors including finance, ICT, public safety, health and e-government services, cybercrime requires a coordinated and comprehensive response. It has become apparent that criminals can easily operate across borders and without international cooperation, it would be difficult to investigate, let alone prosecute them.

By acceding to the Convention, a country can benefit from increased cooperation with other signatories and enhance its abilities to investigate and prosecute cybercrimes.

Given all of that, the OSC submits the following recommendation:

1. Fiji accede to the Convention without any reservations;
2. Fiji carefully consider and amend relevant national laws, including the Online Safety Act 2018, to work coherently rather than in isolation; and
3. Fiji clarifies the role and responsibility of existing law enforcement and State agencies in relation to this Convention.

Thank you, Mr. Chairman. If there are any questions, we are here to answer.

MR. CHAIRMAN.- Thank you, Ms Devi, for that submission. I now open the floor to honourable Members, if there are any questions.

HON. J.R. VOCEA.- Mr. Chairman, through you, the OSC is the only establishment in the country where you can lodge a report regarding online bullying, image-based abuse and other related forms of online abuse. Can you just update the Committee on the situation in Fiji - the amount of reports you are your receiving daily or weekly and other activities related to cybercrime in Fiji? What is the magnitude or nature of the reports that you are receiving in the Commission?

MS. T. DEVI.- Mr. Chairman, it is actually a very good question because the fact that since our establishment in 2019, we have seen an increased number of complaints. We have received 3,000 plus complaints till date from 2019.

Noting that, the number of complaints that we have been receiving till date to be the highest in statistics, I would say, would be defamation so, more to defamatory comments opposed that is happening on the social media platform, especially on the *Facebook* platform, noting that majority of the population in Fiji are on *Facebook*. Now, increasingly, they are shifting to the *TikTok* platform so a lot of complaints that the OSC is receiving are the videos that are created on the *TikTok* platform.

The nature of the complaints mostly are cyberbullying, so that is increasing due to the videos that are being created on *TikTok*. Image-based abuse has a low percentage, however, it is noted that individuals do not want to actually come and lodge their complaint, just because the types of images they would want to share would not be sufficient.

Other than that, it was noted during COVID-19 time that the Commission was receiving a lot towards online gaming, just because the students were at home so they were mostly playing games online. So online gaming was reported the highest during the COVID-19 time.

Online harassment and hacking of accounts was also reported. Few of the reports that did not fall under the OSC jurisdiction was referred to cybercrime or any relevant authorities who may look into those matters. Others being, buying and selling online, so this is where they try to buy something online and they do not get the item, which they pay for.

This year, we have seen a lot of scamming that is going on online. This is where people would call you or something like investment scam on the social media platforms. So, people would try to offer you some amount of money and even ask you to pay for registration fee and people have actually paid for those but have not got any return. Those are the types of complaints that we have received as of now.

HON. I. NAIVALURUA.- Mr. Chairman, through you, I have noted the functions and roles of quite an important establishment. My first question is really how big is the establishment or how are you structured? Are you able to handle the work that you are required to do?

Secondly, just to expand a bit more on the question by my colleague, honourable Vocea, just a simple understanding on the number of cases that have proceeded into court and if it is in court, whether it was successfully prosecuted?

MS. T. DEVI.- Mr. Chairman, if I may answer the first question in terms of the work and the workflow that is happening with OSC, we are able to co-operate just because we have signed the Memorandum of Understanding with the Fiji Police Force and they are absolutely very helpful to us in assisting in any way possible.

We have, sort of, aligned our workflow in a way that complaints are handled efficiently and also if we are not able to investigate any matter, we do refer them to the Fiji Police Force.

In terms of prosecuting matters or matters that have been taken to the court, there are few matters that were taken to court but we had to refer those matters to the Fiji Police Force, considering that the OSC cannot prosecute matters, so it went through the Fiji Police Force. If you may, then we can always provide statistics as a form of written response so that you have a fair idea on the number of cases were taken to court and what exactly is happening right now.

MR. CHAIRMAN.- Just a follow on question from honourable Vocea. When you receive complaints from an individual or an organisation, can you just explain very briefly what happens after that?

MS. T. DEVI.- Mr. Chairman, for instance, if someone is lodging a complaint, there are means to actually to lodge a complaint, either through e-mail, website or phone call or face to face if they want to visit us. As soon as we receive a complaint, the first thing is asking all the details of the complainant or asking them to fill out the form that was actually gazetted. They fill that form requiring all the details of the complaint, and once the details are taken, depending on the nature of the complaint, if I may explain a type of complaint, for instance, image-based abuse.

We have actually escalated our pathways or have a very good relationship with the platforms *Meta* and *TikTok*. So depending on the nature of the complaint, we ask for evidences. In the case where it is image-based abuse, we do not ask for the images. This is where we have liaised with the *Meta* and we, sort of, have that relationship with them in terms of having that link to actually provide the complainant with which is called Non-Consensual Sharing of Intimate Images. That is where we send that link to the complainants, they will have to upload those

pictures on that link. What Meta does is, before the post, for instance, if someone is threatening to post, those pictures are to be uploaded on that link. What happens next is, Meta will actually hash those photos from being posted online. That is for image-based abuse.

Secondly, if it is being shared through *Viber* or *Whatsapp*, that is something that we cannot actually control, so we get the details of the alleged perpetrator and forward it to the Cybercrimes Unit for further investigations because, obviously, with *Viber* and *Whatsapp*, we can get the phone contact and also where they can track the person down or just get the details of the perpetrator. Then the matter is referred to them.

If it is continuous, then obviously we send a notice of removal to the alleged perpetrator. This is something which we can do and this is how the notice of removal works. We will send them this notice to actually remove the pictures or any links or posts from the device or from any social media platforms. If they do not comply within the stipulated timeframe that we give, then we can take the matter further with the Cybercrimes Unit.

In the case where it is just cyber bullying, we request for links, so they are to provide us with the links. Sometimes when some of the complainants lodge a complaint, the post is already deleted from the platform, but they take a screenshot to report. However, we cannot assist in that matter but the only thing we can do is to provide them with advice. For instance, if it is posted up again, then they can report it to us but in the case if that link is still active, we send them some reporting mechanisms. For example, if it is reporting an impersonating account, then we send them that link to actually follow the instructions to report directly to the platform. So, if they report to the social media platforms, they definitely send a response whether they can remove that link or not, so either way, they take a screenshot and send it to us. What we do is, if it is not removed, then we send it directly to the platforms for removal.

MR. CHAIRMAN.- You have forensic capability within the Commission?

MS. T. DEVI.- Unfortunately, no, so that is why we do take assistance from the Cybercrimes Unit.

MR. CHAIRMAN.- This is a hearing on the Budapest Convention, but I ask that question because this is an opportunity also for the members of the public who are listening to have an idea of what you do and how they can get in touch with you when it comes to the bullying and all those bad things that are happening in cyberspace. Signing up to this Convention allows us to connect with the other countries who are leaders really in this fight against cybercrime - those that are really looking into cyberspace and trying to, as much as they can, help make it a safe space for what cyber is supposed to be doing in a positive way to us. So, it allows for that coordination with those big countries and I think they also allow for a bit of capacity building.

With that in mind, with the current status of the OSC, is there any need that you have right now that you are looking at that you do not have that would make your Commission much better, more efficient, more effective in the work that you do? It is a general question. On your capacity, is there anything that you would want? If I can put it in a more hypothetical way, Ms. Devi, if you have a magic wand and you get to wave it once and say, "This is what I will have for the Commission", what would it be?

MS. T. DEVI.- Thank you, Sir. It is actually a very good question because there are few things:

1. Staff members of the OSC. Since its establishment, we are only a few staff - less than 10, so I may say less than 5, and we have been operating the Commission since then. However, we have parted ways in terms of, we can say that we are a complaints team but only one person is there in the complaints team to handle so many complaints. So, we are looking into that with the current budget. We will try to sort that out, in a way that we try to still structure the Commission in a way that everyone has their role to play.
2. You may have seen that the Online Safety Act 2018 has not been reviewed till date, so we are looking into that as well this year because the time it was enacted it was not practically used in Fiji. So, now that we know what is happening, what needs to be done and what has to be done, those can be effected on the Act. So, the major part is reviewing the Act which is pending, and we are working towards reviewing that.
3. I feel that this Convention is more on criminal-related offences, however OSC can play a role in terms of creating awareness and helping enforcement agencies, such as the Fiji Police Force, to implement it. Thank you, Sir.

HON. I. NAIVALURUA.- Mr. Chairman, through you, I noted in your brief, Ms. Devi, that you have highlighted an area of concern that women and girls are targeted online. Is it also part of your function or role that you advocate and educate the Community on how they can defend themselves on what to do and what not to do? Do you also do that?

MS. T. DEVI.- Yes, we do. Actually, in partnership with the Office of the e-Safety Commission in Australia - the other agency in the world, we are working on the online gender-based violence so this is where we are creating resources. What we have seen is, most statistics say that women are mostly targeted. What happens is, we are working towards engaging with the e-Safety Commission in terms of getting resources so that we are able to go out to the communities or to these certain women's groups to create awareness sessions in terms of how they can defend themselves online. This may include increasing their digital literacy level as well.

HON. I. NAIVALURUA.- If I may again, Mr. Chairman, through you, I draw your attention, Ms. Devi, to your second recommendation on the Online Safety Act. The Committee would be interested, especially for me, to know whether there is one or two particular part of the Act that you need to review, could you, please, explain or highlight it to us?

MS. T. DEVI.- In terms of section 3 of the Online Safety Act - Objectives, it says that the OSC can only look into matters such as online bullying, internet trolling, cyber stalking and image-based abused. We want to, sort of, expand that because with cyberbullying, it says, "in respect of children". However, adults face more of the abuses online as well. So, it, sort of, expands it more to include adult abuse or any other form of abuses that the OSC has received till date.

MR. CHAIRMAN.- I just go back to that issue that honourable Naivalurua raised. The sad thing is, women and children are disproportionately targeted on the cyberspace. Today in Parliament, we call it “black Thursday”, and you see everyone wearing a bit of black on their clothes. It is really to remember those victims of abuse.

I know that the cyberspace is creating that space for a lot more and then what we are facing. Now, that you are here, and given that this is a public hearing for people who are listening, they know that there is a place that they can go to, that is, the OSC if they are facing all these bullying and this is an opportunity also to raise that issue with those who are listening in today.

Honourable Members, I see that they are all staring at me, and I think that is it. Mr. Siwatibau, would you like to contribute? Thank you.

MR. S.S. WAQA.- Thank you, Mr. Chairman, and honourable Members, if I would just enlighten the Committee on the role of the OSC, throughout the years as we have known that this is the only OSC that looks into online crimes that are established in Pacific Island Countries. So, there has been discussions in replicating this (OSC) to other Pacific Island Countries and they are looking towards Fiji as a symbol of Online Safety Advocacy in the region.

In terms of addressing the issues of online abuses, the OSC, together with other stakeholders, have put out resources in all languages, both the vernacular in the *iTaukei* and also in the Hindi language, as well as in English, that are usually shared with the communities that we go and conduct awareness to. We have also partnered with the Fiji Police Force in raising awareness and we do this on all the media platforms that are available, and also upon invitation from individual communities.

In regard to the ongoing aspect of trying to enhance the OSC’s duty into protecting the citizens of Fiji from online harm, we are recommending to the honourable Minister to review the Online Safety Act and that is just to encapsulate the current trend of online crimes that evolve with evolving technologies. As technologies evolve, the crime trend also evolves with it, and we are trying to get our laws on the Online Safety Act to also be able to protect our citizens from this evolving crime. And that is we thank the team at the OSC and also the other stakeholders that support the Commission. I am a member of that Working Group that usually works together with the OSC in addressing issues that are reported to the Commission. Thank you, Sir.

MR. CHAIRMAN.- Thank you. Yes, honourable Vocea.

HON. J.R. VOCEA.- Mr. Chairman, through you, just a quick question in regards to your awareness campaign, especially to our youth in schools. These are the more vulnerable ones. How are you going on with your campaign to schools and the youth population in terms of these cybercrime activities?

MS. T. DEVI.- Mr. Chairmam, if I may, this year, we celebrated the Safer Internet Day 2023 which is usually celebrated throughout the Globe on Tuesday, 7<sup>th</sup> February, 2023.

What happens on this day is you focus on a topic and you use it for the whole of the year to advocate or raise community awareness. So, this year, the OSC decided to focus on the youth so we actually just started with collaborating with the Universities and we are going out to their relevant Campuses to actually raise awareness.

We came up with this Online Safety Champions Programme where we are collecting few students, trying to form a club in each of the Campuses, and we are going to train them with all the different types of issues that the OSC is receiving. We are going to certify them so that they can advocate in their relevant Campuses, on behalf of the OSC, in terms of what is happening online, how they are behaving online, the languages they use, so all these are covered in that Online Safety Champions Programme.

With regards to working with the schools, we are currently trying to figure out ways to relate with the Ministry of Education so that we can go out to schools and also create awareness. However, we have already been to a few of the schools with the online safety booklets that we launched in 2022. Those are for the parents and children, so those books were already distributed to the schools. But we are now going out to the schools to actually see whether they have been reading those books or whether they have any knowledge of those books. So, over 40,000 booklets were distributed to the schools and communities. Thank you.

MR. CHAIRMAN.- Thank you, Ms. Devi. One quick question from me, last year was Elections year. Did you see a corresponding increase when it comes to election years on online abuses, bullying, et cetera?

MS. T. DEVI.- Yes, Sir. Online bullying was happening. As I had mentioned earlier with regards to youth or adults actually creating videos on the platform *TikTok*, however, a lot were noted in terms of defamation. So, statistics say that a lot have been received by the Commission on defamatory comments and posts.

MR. S.S. WAQA.- Just to add on to that, Sir, last year, we also held a workshop with women Parliamentarians because we noticed that they are the most vulnerable ones, who are usually targeted online. We taught them on how to protect themselves and how to respond to online bullying.

With that also, in regards to honourable Vocea's question on awareness raising, we have other advocates who believe in raising awareness to protect communities and we currently have an agreement with the Film and Television Unit. We are proud that they are supporting us on this.

They have dedicated a season of television show - talkback show to us, in raising awareness in the *iTaukei* language and this can be viewed this afternoon - every Thursday at 7.30 p.m. The programme is called *Dou Mada Mai* and we use all types of media and platforms to raise awareness in regards to online safety and it is an ongoing issue, Sir, with the current evolving technology and a lot of accessibility.

As we can understand, Fiji is one of the cheapest countries to have internet access and this is a challenge, in itself, that a lot of people use this accessibility to create harm online. So, we would like to educate them with the use of digital literacy education materials to a more productive and more efficient way for them to enjoy

technology as it was supposed to be and with that, we are very glad that we have the support of many other advocates.

There was an NGO from a Commonwealth country called 'Get Safe Online' that has created a Fijian vernacular website, 'Get Safe Online Fiji' in the vernacular version, just to enable people who need materials and resources and who have questions, to get online, type into Get Safe Online Fiji website and they will have the materials in Fijian, *iTaukei* and also in English.

Those are the types of awareness raising that the OSC, together with the Fiji Police Force and other NGOs are using to address these important issues in Fiji. Thank you, Sir.

MR. CHAIRMAN.- Ms. Devi, do you have any final words for us.

MS. T. DEVI.- Thank you, Mr. Chairman and honourable Members. I do not have any final comments, however, if there are any other questions, we are happy to answer because I know this is the platform where all the questions and answers are important, and you are able to get all the information as much as possible from the OSC.

HON. J.R. VOCEA.- Just one question, do you have any counsellor in your team to deal with your staff when you are receiving the complaints and reports everyday?

MS. T. DEVI.- We do not have a counsellor, Sir. However, we liaise very closely with the Fiji Women's Crisis Centre so we have, sort of, forged that relationship where our staff can easily walk in and try to debrief themselves.

MR. CHAIRMAN.- If there are no other questions from honourable Members, let me just express our sincere appreciation to Ms. Devi and Mr. Waqa. Thank you for coming in today to present to us.

As I had mentioned, this is a hearing on the Budapest Convention - Convention on Cybercrime that Fiji is wanting to accede to. Thank you for the recommendations that you have given to us - the three very clear recommendations according to that Convention.

However, we have valued-added this hearing a little bit, given we are talking about cybercrime, to allow you the opportunity and allow all those who are listening - our viewers, to have a fair understanding of the OSC. For those who are facing the negative effects of the cyberspace that we are trying to deal with, they can come in and lodge their complaints with you and on behalf of the Committee, we would like to thank you for the work that you do. Thank you for coming in today to present to us and I hope that you will avail yourselves if the Committee has any further queries on this matter that we are dealing with today.

On that note, thank you, honourable Members and our submittees, for your time today. *Vinaka va'levu*. I will now declare the meeting closed. I think there is morning tea prepared and we can invite you to have morning tea with us, if you have time.

The Committee adjourned at 9.40 a.m.

# **[VERBATIM REPORT]**

## **MEETING OF THE S/C ON FOREIGN AFFAIRS & DEFENCE**

### **CONVENTION**

**Convention on Cybercrime (Budapest Convention)**

**INSTITUTION: Ministry of Home Affairs and  
Immigration**

**VENUE: Big Committee Room (East Wing)**

**DATE: Thursday, 13<sup>th</sup> April, 2023**

**VERBATIM REPORT OF THE MEETING OF THE STANDING COMMITTEE ON FOREIGN AFFAIRS AND DEFENCE HELD IN THE BIG COMMITTEE ROOM (EAST WING), PARLIAMENT PRECINCTS, GOVERNMENT BUILDINGS, ON TUESDAY, 2ND APRIL, 2023 AT 9.54 A.M.**

**Interviewee/ Submittee: - Ministry of Home Affairs and Immigration**

**In Attendance :**

1. Mr. Manasa Lesuma - Permanent Secretary
  2. Mr. Jemesa Lave - Police Secondment Officer
  3. Mr. Savenaca Siwatibau - Police Secondment Officer
  4. Mr. Lorima Sautu - Police Officer
  5. Mr. Mesake Sovasova - Police Liaison Officer
- 

MR. CHAIRMAN.- Honourable Members, members of the public, the Secretariat and ladies and gentlemen; a very good morning to you all. It is a pleasure to welcome everyone, especially the viewers who are watching this proceeding.

This is a meeting of the Standing Committee on Foreign Affairs and Defence. At the outset, for information purposes, pursuant to Standing Orders of Parliament, specifically Standing Order 111, all Committee meetings are to be open to the public. Therefore, this meeting is open to the public and the media and is also being streamed live on the Parliament *Facebook* page and the Parliament Channel on the Walesi platform.

For any sensitive information concerning this submission that cannot be disclosed in public, that can be provided to the Committee either in private or in writing, but do note that this will only be allowed in a few specific circumstances which include:

1. National Security matters;
2. Third party confidential information;
3. Personnel or human resources matters; and 4. Committee deliberation and development of Committee's recommendation and report.

I wish to remind honourable Members and our invited guests that all comments and questions are to be addressed through the Chairman. This is a parliamentary meeting and all information gathered is covered under the Parliamentary Powers and Privileges Act and the Standing Order of Parliament.

In terms of other protocols of this Committee meeting, please, be advised that movement within the meeting room will be restricted. please, minimise the usage of mobile phones and all mobile phones to be on silent mode while the meeting is in progress.

(Introduction of Members of the Standing Committee, the Secretariat and Hansard)

With us this morning, we have the representatives of the Ministry of Home Affairs and Immigration, who had been requested to provide a submission on the Convention on Cybercrime. For the purpose of the viewers who are joining us this morning, allow me to give a brief explanation on the Treaty.

The Convention on Cybercrime, also known as the Budapest Convention, provides a comprehensive and coherent framework on cybercrime offences and electronic evidence. It serves as a guideline for any State that is developing a comprehensive national legislation against cybercrime, and as a framework for international cooperation amongst State Parties. To-date, the Convention has 67 Member States, which includes Australia and Tonga from the South Pacific Region.

Pursuant to Article 37 of the Convention, any other State, such as Fiji, can become a Party by accession, if the State is prepared to implement the provisions of the Convention and upon invitation to accede to the Convention after the consultation and approval of the Parties.

With the extreme effects of global cyber threats and attacks on critical sectors, such as finance, ICT, energy, water, emergency services, public safety, health, public services, aviation and e-government infrastructure, becoming a Party to the Convention will enhance Fiji's ability to combat cybercrime, with international support and assistance, particularly, in relation to continued capacity building, to better equip Fiji's criminal justice authorities, including the judiciary, prosecution and law enforcement agencies.

I now take this time to invite our guests to introduce themselves before we proceed with the submission. Please, note that if there are any questions by Members of the Committee, they may interject or we will wait till the end of your submission.

MR. M. LESUMA.- *Bula Vinaka*, Mr. Chairman and honourable Committee Members. I am, indeed, pleased, this morning to be here in person to present to this Committee on the Ministry of Home Affairs and Immigration's comments on the Cybercrime Convention, also commonly known as the Budapest Convention. With me this morning is the Police Liaison Officer, Mr. Mesake Sovasova, and two of our Secondment Officers from the Fiji Police Force, who are Digital Forensic Officers who are now currently based with our Policing Division in the Ministry of Home Affairs. I hope their presence today will help clarify some questions that may arise from our presentation this morning.

Mr. Chairman, as you all may be aware, and as alluded to by Mr. Chairman, the Budapest Convention was opened for signature in Budapest, Hungary, in November 2001, and has been a shared international norm

and law as a means for criminal justice response to cybercrime. For Fiji, the passing of the Cybercrime Act 2021, saw the alignment of our national legislation with the provisions and obligations as set up in the Budapest Convention.

Technological advancement has exponentially grown, and this is evident in its multifaceted use across all sectors, whilst this ensures seamlessly that we do business and general conduct for business processing, it also carries the opportunity for cyber-related crimes to increase. These underscores the importance for Fiji as an upstanding international community partner to accede to the Budapest Convention.

I believe you have copies of the presentation, Mr. Chairman and honourable Members. On the third slide, our presentation will cover the scope that you have on the slide before you. I will start with the background of the work conducted by the Ministry of Home Affairs, particularly, the progress on the Ministry's initiative in the space of cyber security and cybercrime.

We will also introduce a short summary of the Convention. I believe that you all have been thoroughly briefed on the background, the intent and the provisions of the Convention, so I will focus my submission on its security implications.

We will also very briefly highlight Fiji's status so far as the Budapest Convention is concerned, and we will further highlight the details outlining the purposes and the justifications for Fiji to accede to the Budapest Convention.

As a way of background, on slide four, Mr. Chairman and honourable Members, in the late 2010, a cyber security working group was initiated by a group of individuals from the Ministry of Defence, the Fiji Police Force Cybercrime Unit, Telecom, Vodafone, FINTEL, BSP and Westpac. The focus of which was to address issues within the cybersecurity environment of Fiji.

In 2011, a Cabinet paper was submitted to Cabinet and the Cabinet decision was endorsed on the following:

1. Agreed that the working group comprising of the public and private sector stakeholders conduct an empirical research, analysis assessment and make recommendations to the Ministry of Home Affairs on the status of cyber security in Fiji.
2. Working Group to consult with the Office of the Solicitor-General on the development of a legal framework for cyber security and the inception of Fiji's Computer Emergency Response Team (CERT) to monitor and report activities of cyber-related crimes to the Fiji Police Force.
3. A drafting of a law of cybersecurity in consultation with the Office of the Solicitor-General and noted that once drafted, the law will be brought back to Cabinet for its approval.

This formed the basis for the Ministry of Home Affairs' work in cybersecurity. However, in 2019, this was shifted under the previous administration, to the Ministry of Communications where it currently is at the moment.

Moving on to Slide 5, honourable Members, the Budapest Convention provides a framework that outlines common standards in the cybercrime environment. The Convention comprises of four Chapters and 48 Articles, which cover fundamental components of response to criminal activities in cyberspace. Article 36 to Article 48 contains the final provisions, while Article 1 to Article 35 contains the main parts of the Convention in the three areas:

1. Criminalizing activities against and by means of computer or any electronic device.
2. The procedural law tools associated with the investigation of cybercrimes and the acquisitions of electronic evidence.
3. International cooperation on cross jurisdictional matters in cybercrime investigations and electronic evidence.

Recently, there is a propagated move towards capacity building to reinforce criminal justice capabilities on cybercrime. Furthermore, the Convention also provides a framework in which acceding Parties can be guided towards achieving a standardised and uniform legislation which encourages cooperation between State Parties.

On Slide 6, Mr. Chairman and honourable Members, regarding Fiji's status, in 2021, Fiji was invited by the Council of Europe to accede to the Budapest Convention. However, Fiji had several legislations which had adopted some of the provisions of the Budapest Convention, although we have not acceded. We noted that there were few legislations that had adopted some of the provisions. These legislations are the Juvenile Amendment Act 1997, Post and Telecommunication Decree 1989,

Crimes Act 2009 which contains 10 sections under the computer offence, Section 336 to Section 346 and the Cybercrime Act addresses cybercrime via stipulating computer-related and contact-related offences, including procedural requirements, collection of electronic evidence and international cooperation.

The above four legislation, honourable Members, have adopted Articles 1 to Article 22 and Article 24 to Article 35. Now, we noted that there are 48 Articles altogether.

On Slide 7, Mr. Chairman and honourable Members, as I had alluded to earlier in the presentation, the Budapest Convention covers the main fundamental components of law enforcement, response to illegal activities by means of computers and electronic devices and the extension of these activities into cyberspace.

Fiji's acceding to the Budapest Convention would entail the following benefits:

1. It will appropriate the relevance of cybercrime laws to illegal cyber activities which is a challenge of any Nation State. An active cybercrime law is to appraise the dynamic evolving

nature of technology and the internet and enact laws that meet the threshold of this cyber dynamic environment. Small Island Developing Nations such as Fiji, will have access to and benefit from the evolution of the Budapest Convention now and into the future, as a base or platform for reviewing its cyber laws and regulations governing the illegal activities in cyberspace.

2. It would, through capacity building and international co-operation, Fiji will be in a favourable position to better equip its law enforcement, investigative prosecutorial and judicial functions.
3. With international co-operation comes with international standards. Again, should Fiji accede to the Convention, it would also entail compliance with international standards, law enforcements, agency services in the areas of cybercrime investigations and prosecutions and will also need to align with international standards and best practices. This will strengthen and enhance the quality-of-service delivery by law enforcement and prosecutions.

The nexus between cybercrime and cybersecurity on Slide 8 before you, honourable Members, I wish to highlight the important position that cybersecurity holds as an overarching agenda over cybercrime. Now, cybersecurity is all about the various methods and technologies, processes frameworks, policies, strategies and legislation to help protect systems, the networks against cyberthreats and attacks in cyberspace.

Cybercrime refers to criminal activities that are committed using the internet or other forms of digital communication. Cybersecurity is essential for preventing and detecting cybercrime. Without proper cybersecurity measures in place, cyber criminals can easily gain access to computer systems and networks, steal sensitive data, cause significant damage and, in turn, cybercrime can highlight the vulnerabilities and the weaknesses in all organisations. Cybersecurity practice prompting the need for stronger security measures.

Mr. Chairman, and honourable Committee Members, measures must be integrated into national security strategies and policies to ensure that the country is adequately prepared for any cyber threats. In this era of new innovative technology, cybersecurity has become a top priority for national security. The Government must take proactive measures to protect the country's cyber infrastructure, prevent cyber-attacks, respond promptly and effectively to any cyber incident. Cyber security measures must be integrated into the national security strategies and policies and legislations, to ensure that the country is adequately prepared for any cyber threat and to protect the safety of our citizens in cyberspace.

In many countries, Mr. Chairman and honourable Members, the Ministry of Home Affairs and Immigration is responsible for maintaining the law and order, including the prevention and detection of cybercrime.

Cybercrime legislation is a deterrence and a reactive instrument with which government, through law enforcement, ensure that retribution is executed against organised criminal activities in cyberspace. Therefore, cybercrime legislation enforced by the law enforcement is an essential response to cybersecurity threats and breaches in cyberspace.

Honourable Members, in order to combat cybercrime effectively in Fiji, the Ministry of Home Affairs and Immigration may enhance existing machinery within Government that will assist in investigating and prosecuting cybercrime cases and may work effectively in collaboration with other law enforcement agencies and international partners.

Therefore, the Ministry of Home Affairs and Immigration plays an important role in addressing the growing threat of cybercrimes which has become an increasingly complex and sophisticated problem in today's digital age. Maintaining strong cyber security measures is critical for preventing cybercrime and protecting the individual organisation and society from the negative impacts of cyber-attacks. It is crucial, honourable Members, to align cybercrime legislation and cyber security with national security and recognise its importance in this era of new innovative technology.

Mr. Chairman and honourable Members, Fiji acceding to the Budapest Convention would not only strengthen Fiji's retributive security mechanisms to threats in cyberspace, it would also greatly benefit cyber-related security thematic areas under the Ministry of Home Affairs and Immigration, such as the critical infrastructure.

The Ministry of Home Affairs and Immigration is mandated in providing policy guidance on critical infrastructure security platforms to ensure a safe and secure Fiji for all. So critical infrastructure describes the physical or virtual assets or services that are essential for the functioning of society and the economy.

Critical infrastructure is so vital that its impediment or destruction would inflict a rehabilitative impact upon our physical or economic security or public health or safety. Any physical or virtual assets or services that is deemed as critical infrastructure is of national importance.

Critical infrastructure, honourable Members, is increasingly inter-related and interconnected, delivering the efficiencies and economic benefits to the two operations. However, connectivity without proper safeguards creates vulnerabilities that can deliberately cause disruption that could result in cascading consequences across our economy, security and sovereignty.

The Ministry of Home Affairs and Immigration, honourable Members, is currently working together with other government and public and private stakeholders in the development of a proposed National Critical Infrastructure Cyber Incident Response and Recovery Framework to protect Fiji's critical infrastructure from all hazards, including the dynamic and potentially catastrophic cascading threats enabled by cyber-attacks.

This proposed Framework, honourable Members, will incorporate Critical Infrastructure Computer Emergency Response Team (CICERT) and a Critical Infrastructure Computer Security Incident Response Team (CICSIRT). Designated information security experts will form the CICERT and is primarily responsible for the protection against detection of, and respond to cybersecurity incidents within the critical infrastructure community.

The CICSIRT will consist of information security experts within each critical infrastructure organisation, whose main goal is to respond to critical infrastructure computer security incidents quickly, effectively and efficiently, thus regaining control and minimising damage.

Parties to the Budapest Convention would, of course, open opportunities to receive and share invaluable information of pervasive threats in cyberspace which would best be utilised by the CICERT and the CICSIRT Teams for awareness and proactive protection initiatives within the critical infrastructure community.

Fiji's acceding to the Convention would further enhance the response components of the National Critical Infrastructure Cyber Incident Response and Recovery Framework through international cooperations and collaborations with parties to the Convention.

From a response and retribution stance, cyber threat incidents within the critical infrastructure community requiring law enforcement response would be effectively and efficiently addressed through access to international cooperation mechanisms and capacity building.

Slide 10, Mr. Chairman and honourable Committee Members, talks about the reassignment of cybercrime legislations to the Ministry of Home Affairs and Immigration. In many countries, maintaining law and order frequently falls under the purview of the Ministry of Home Affairs, which includes preventing and identifying cybercrime.

The Fiji Police Force began the cybercrime investigation and computer forensic capability through an international money laundering case in 2006. Since then, the Cybercrime Unit of the Fiji Police Force has grown, to the recent inception of its first digital forensic laboratory in October 2022.

To successfully combat cybercrimes in Fiji, the Ministry of Home Affairs and Immigration through the Fiji Police Force may enhance existing Government machinery that will assist in investigating and prosecuting incidents of cybercrime. It may also successfully collaborate with other law enforcement agencies and outside partners.

In 2009, Mr. Chairman and honourable Committee Members, the Crimes Act replaced the Penal Code. The Crimes Act has 10 sections under computer offences, and the Fiji Police Force Cybercrime Unit processes reports that certain allegations or breaches within the computer offence sections of the Crimes Act.

Through the Ministry of Home Affairs and Immigration, strategies and plans to combat cybercrime can be developed, such as enforcing laws to ensure businesses protect their digital systems from cyber threats and carrying out public awareness. Additionally, the Ministry works with Government and international agencies to protect information and collaborate on initiatives to combat cybercrime at regional and international levels. Therefore, the Ministry of Home Affairs and Immigration plays an important role in addressing the

growing threat of cybercrime which has become an increasingly complex and sophisticated problem in today's digital age.

Mr. Chairman and Committee Members, the Fiji Police Force Cybercrime Unit not only limits itself to cybercrime investigation, but it is also heavily involved in other areas that are related to the effect of threats in cyberspace, such as online safety, internet cyber awareness programmes, cyber security and the protection of citizens from the harms of internet.

In view of the above, we are trying to propose the support from this Committee to transfer the Cyber Crime Act 2021 to be under the portfolio of the Minister for Home Affairs and Immigration, given that the Fiji Police Force is under the ministerial assignment of the Minister for Home Affairs and Immigration and considering that prime effect, that the response to breaches in cyberspace through investigations of cybercrimes are handled by the Cybercrime Unit within the Fiji Police Force.

Mr. Chairman and honourable Members, Slide 11 highlights the way forward. Considering the security benefits, it is recommended that Fiji accedes to the Budapest Convention. This leverages Fiji's efforts to be on par with international standards on cybercrime retribution and proactive benefits.

Further, to guarantee a safe and secure Fiji for everyone, the Ministry of Home Affairs and Immigration is mandated to provide policy guidance of critical infrastructure security platforms.

In addition to enhancing Fiji's response to security measures to cyberspace threats, Fiji's accession to the Budapest Convention would have a significant positive impact on critical infrastructure and other cyber-related security thematic areas under the Ministry of Home Affairs and Immigration.

Mr. Chairman and honourable Members, the Fiji Police Force, currently, is the only agency that will fully exhaust provisions in the cybercrime legislation. Therefore, it is imperative that the Cyber Crime Act 2021 be assigned to the Minister for Home Affairs and Immigration.

Mr. Chairman and honourable Members, the Ministry of Home Affairs and Immigration thanks the attention of the Committee throughout our submission this morning, and we await any questions and comments.  
*Vinaka saka vakalevu.*

MR. CHAIRMAN.- Thank you, PS and your Team, for your presentation. I now open the floor for questions from honourable Members, if they have any.

HON. J.R. VOCEA.- *Bula vinaka*, Mr. Chairman. I would like to raise a question, please. It is quite enlightening to hear the submission from the Ministry of Home Affairs and Immigration just as we are about to table this motion to Parliament for Fiji to accede to the Budapest Convention.

My question to the Ministry of Home Affairs is, given that we have the Cybercrimes Act, Online Safety Commission Act and the Crimes Act, if we are to accede to the Budapest Convention, do they think that we still need to review some of these Acts to be online, or safeguard us from any other threat as we are the signatory to the Convention? Those Acts that we have the Cybercrime Act, Online Safety Commission Act and the Crimes Act, what is the view of the Ministry of Home Affairs - do we still need to review some components of those Acts?

MR. M. LESUMA.- I believe the Ministry will be working closely with the Office of the Solicitor-General, particularly in the review of the Act. The Articles are pretty clear in terms of what we accede to the Budapest Convention, and we will be taking guidance from the Office of the

Solicitor-General, particularly if there are overlaps in areas that need to be addressed with the current Acts that are currently in place. I believe the Office of the Solicitor-Generals would be the best to address those issues, but we will be working with the Office of the Solicitor-General, particularly in looking at the current legislations that are in place, what would be effected, and how that could be addressed.

HON. J.R. VOCEA.- *Vinaka.*

MR. CHAIRMAN.- For the benefit of the submittees, my understanding of the mandate of this Committee is to look at the Convention in relation to whether we should accede to it or not, as it was tabled in Parliament, but we are in a situation where we have a Cybercrime Act.

Usually, you accede to the Convention and then you write up your legislation. In this case for Fiji, we are thankful that we already have a Cybercrime Act which is very much aligned to the Convention. I think that was done to show our commitment to the Parties that are willing to go along with what is required in the Convention, and I think that is one of the reasons why they are inviting Fiji to accede to the Convention.

I have heard your recommendation. It seems a very logical recommendation to me but it is dealing with the Cybercrime Act on whether it is to remain with the Ministry of Communications or should it be transferred across to the Ministry of Home Affairs.

As I have said, I have seen the logic in it but we can just value add and include in our Report your recommendation that the Cybercrime Act be transferred to the Ministry of Home Affairs. But our mandate is to go back to Parliament and say whether Fiji should ratify the Convention or not, and in that way just value add and include in the Report your recommendation which is a recommendation on the Cybercrimes Act, and it can go on from there and see what needs to be done. That is my comment.

Are there any further questions from honourable Members?

HON. I. NAIVALURUA.- I just wanted to add on to the comments made by Mr. Chairman. The presentation is well understood and well noted and is most logical in our thinking from the security perspective that it be transferred to the Ministry of Home Affairs and Immigration. I thank you for a good presentation this morning. I can say that I agree with Mr. Chairman.

You have convinced us this morning and, in my view, that it is very important for a holistic approach to the implementation and effective strategies put into place and there is got to be changes too, as you have heard from our colleague, that it needs to be done accordingly. So, from my perspective I fully understand that, and it is well noted.

MR. CHAIRMAN.- I just like to add that in the presentations that we have had, one of the recurring questions is, who takes the lead? I think there is a blurring as to who takes the lead when it comes to cybercrime. I guess your recommendation this morning is along those lines and we can clear that up and be more effective and efficient.

Honourable Members, if there are no further questions, I thank the team from the Ministry of Home Affairs - Permanent Secretary and your Team. Thank you so much for coming in this morning and sharing that presentation with us.

I note that you had provided a written statement earlier to the previous Committee regarding the Convention. Please, note what I had mentioned earlier that we certainly will just value add our Report and include in it your recommendation with regards to the Cybercrime Act.

With that, I thank everyone. Honourable Members, I declare the meeting closed. I think there is morning tea, and you are invited to have tea with us. *Vinaka vakalevu.*

The Committee adjourned at 10.32 a.m.

