**CONVENTION ON CYBCERCRIME**

**(BUDAPEST CONVENTION)**

**WRITTEN ANALYSIS**

1. **INTRODUCTION**
	1. The Convention on Cybercrime, also known as the Budapest Convention (‘**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 (**‘Parties’**).
	2. 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.
	3. 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.
2. **SUMMARY OF THE CONVENTION**
	1. The Convention contains a total of 48 Articles.
	2. Article 1 of the Convention provides for the specific definitions of the terms ‘computer system’, ‘computer data’, ‘service provider’ and ‘traffic data’.
	3. Article 2 of the Convention requires each Party to adopt legislative and other measures to establish a criminal offences, when committed intentionally, the access to the whole or any part of a computer system without right.
	4. Article 3 of the Convention requires each Party to adopt legislative and other measures to establish as criminal offences, 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.
	5. Articles 4 and 5 of the Convention requires 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 functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or supressing computer data.
	6. Article 6 of the Convention requires each Party to adopt legislative and other measures to establish as criminal offences, misuse of devices.
	7. Article 7 of the Convention 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.
	8. Articles 8 of the Convention requires each Party to adopt legislative and other measures to establish as criminal offences, when committed intentionally and without right, the causing of loss of property of another person by any input, alteration, deletion, suppression of computer data, any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring without right, an economic benefit for oneself or another.
	9. Articles 9 of the Convention requires each Party to adopt legislative and other measures to establish as criminal offences, offences related to child pornography.
	10. Articles 10 of the Convention requires each Party to adopt legislative and other measures to establish as criminal offences the infringement of copyright and related rights as defined under a Party’s laws.
	11. Articles 11 of the Convention requires each Party to adopt legislative and other measures to establish as criminal offences, when committed intentionally, aiding and abetting the commission of any offence established under Articles 2 to 10, with intent such offence be committed.
	12. Articles 12 of the Convention requires each Party to adopt legislative and other measures to ensure that legal persons can be held liable for a criminal offence under established under the Convention.
	13. Article 13 of the Convention requires each Party to adopt legislative and other measures to ensure that the criminal offences established under Articles 2 to 11 are punishable by effective, proportionate and dissuasive sanctions.
	14. Article 14 of the Convention provides the scope of the procedural measures for the purpose of specific criminal investigations or proceedings.
	15. 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 inter alia public interest and the rights, responsibilities and legitimate interests of third parties.
	16. Article 16 of the Convention requires each Party to adopt legislative and other measures to empower competent authorities to order or obtain 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.
	17. Article 17 of the Convention requires each Party to adopt legislative and other measures ensure expeditious preservation of traffic data is available and is sufficient enough to identify service providers and the path through which communication was transmitted
	18. Article 18 of the Convention requires each Party to adopt legislative and other measures to empower competent authorities to order a person in its territory to submit specified computer data in the person’s possession or control which is stored in a computer system or computer-data storage medium and to order 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.
	19. Article 19 of the Convention requires each Party to adopt legislative and other measures to empower competent authorities to search or access a computer system or part thereof and computer data stored therein and a computer-data storage medium in which computer data may be stored.
	20. Articles 20 and 21 of the Convention requires each Party to adopt legislative and other measures necessary in relation to serious offences to empower competent authorities to collect or record through the application of technical means of that Party and compel a service provider, within its technical capability, to collect or record and to cooperate and assist competent authorities to collect or record, content data and traffic data, respectively, in real-time of or associated with, specified communication in its territory transmitted by a computer system.
	21. Article 22 of the Convention covers jurisdiction. Under Article 22 of the Convention, each Party must adopt legislative and other measures to establish jurisdiction over an offence established in accordance with Articles 2 to 11 of the Convention, when the offence is committed in its territory, on board a ship flying its flag, on board an aircraft registered under its laws, or by one of its nationals if publishable under a criminal law where it is committed or if the offence is committed outside the territorial jurisdiction of any State. It further provides that where more than one Party claims jurisdiction over an alleged offence, the Parties involved must, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.
	22. Article 23 of the Convention outlines the general principles relating to international co-operation through the 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.
	23. Article 24 of the Convention provides for principles relating to extradition. Article 24 of the Convention applies to extradition between Parties for criminal offences established under Articles 2 to 11 to the Convention, provided the offences 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. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniformity or reciprocal legislation or an extradition treaty, the minimum penalty provided for under such arrangement or treaty applies.
	24. Article 25 of the Convention provides the general principles relating to mutual assistance which include mutual assistance to the widest extent possible 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, 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 25 of the Convention also provides that mutual assistance must be subject to conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including grounds for on which the requested Party may refuse co-operation. It also addresses the issue of dual criminality.
	25. 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. Forwarding such information however may be subject to the condition that the information be kept confidential or be used subject to conditions, which the receiving Party can decide to accept and be bound by.
	26. 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 made. Each Party must designate a central authority or authorities responsible for sending and answering requests for mutual assistance, execution of such requests or transmission to authorities competent for their execution. Mutual assistance requests must be executed in accordance with procedures specified by the requesting Party unless incompatible with the law of the requested Party. Where such treaty or arrangement exist, Article 27 of the Convention does not apply unless the Parties concerned agree to its application.
	27. 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 requested Parties, for the supply of information on the condition that it is kept confidential or not used for investigation other than those stated in the request. Where such treaty or arrangement exist, Article 28 of the Convention does not apply unless the Parties concerned agree to its application.
	28. 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 and for which the requesting State is intending to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. The requested Party must take all appropriate measures to expeditiously preserve the specified data in accordance with its domestic laws. Dual criminality is not a condition to the providing preservation of the requested data.
	29. 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 is 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 its sovereignty, security, ordre public or other essential interests.
	30. 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. The requested Party must expeditiously respond where there are grounds to believe that the relevant data is particularly vulnerable to loss or modification or where the instruments, arrangements and laws used to respond to such requests otherwise provide for expedited co-operation.
	31. Article 32 of the Convention allows a State Party, without authorisation of another State Party to access publically 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 Party, provided the lawful and voluntary consent of the person who has lawful authority to disclose the data through that computer system is obtained.
	32. Articles 33 and 34 of the Convention require Parties to provide mutual assistance to each other in:
3. real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system; at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case and under domestic law; and
4. 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.
	1. Article 35 of the Convention requires each State Party to designate a point of contact on a twenty-four hour, seven-day-a-week basis, 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. Under Article 35 of the Convention, a State Party must ensure that trained equipped personnel are available to facilitate the operation of the network.
	2. Article 36 of the Convention provides for the signing of the Convention by member States of the Council of Europe and by non-member States which participated in its elaboration, as well as for when the Convention enters into force for such States. Article 36 of the Convention also provides for the ratification, acceptance or approval of the Convention where instruments of ratification, acceptance or approval must be deposited with the Secretary General.
	3. Article 37 of the Convention provides the process for accession to the Convention. The Committee of Ministers 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. The Convention will come into force for a State acceding to the Convention 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 Secretary General.
	4. 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. 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. 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.
	5. 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 on 13 December 1959 (ETS No. 24), the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasburg, 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 Strasburg on 17 March 1978 (ETS No. 99). Where an agreement or treaty has already concluded or relations established, Parties are also entitles to apply the agreement or treaty or regulate such relations in a manner that is not inconsistent with the Convention.
	6. 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 Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27 paragraph 9.e, by written notification to the Secretary General.
	7. Article 41 of 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 co-operate under Chapter III. 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. 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.
	8. Article 42 of 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.
	9. Article 43 of 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. Article 43 of the Convention also allows the Secretary General to periodically enquire with Parties who have reservations as to the prospects for withdrawing their reservations.
	10. Article 44 of the Convention provides the means through which any amendment to the Convention may be proposed by any Party i.e. communicated by the Secretary General to member States, non-member States which have participated in the elaboration of the Convention and any State which has acceded to, or has been invited to accede to the Convention. Any amendment to the Convention must also be communicated to European Committee on Crime Problems (CDPC), which must then submit its opinion on the proposed amendment to the Committee of Ministers. Following consultations with non-member Parties of the Convention, the Committee of Ministers may adopt the amendment, the text of which will then be forwarded to Parties for acceptance. Any adopted amendment comes into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance of the amendment.
	11. Article 45 of 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.
	12. Article 46 of 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. 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.
	13. Article 47 of 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.
	14. 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, 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.
5. **REQUIREMENTS FOR IMPLEMENTATION**
	1. Obligations of Parties to the Convention are expressly stated under Chapter II of the Convention which specifies measures that need to be taken at the national level including the adoption of legislative and other measures:
6. Articles 2 - 13 : substantive criminal law offences;
7. Articles 14 – 21 : procedural law; and
8. Article 22: jurisdiction.
	1. Other obligations of the State include the appointment of the relevant authority responsible for sending and answering requests for mutual assistance (Article 27) as well as a 24-hour network contact (Article 35)
	2. This means that Fiji must, in addition to having legislation that meets the requirements of the Convention i.e. the Cybercrime Act 2021, ensure that other mechanisms and safeguards are put in place to ensure that the Convention is fully implemented. Introducing review mechanisms would also help improve processes when dealing with mutual assistance requests.
9. **IMPACT OF THE CONVENTION**
	1. Becoming a Party to the Convention entails the following advantages for Fiji:
10. the Convention provides a legal framework for international cooperation on cybercrime and electronic evidence. Chapter III of the Convention makes general and specific provisions for international cooperation among Parties not only with respect to cybercrime offences against and by means of computers but with respect to any crime involving electronic evidence;
11. Fiji as a Party to the Convention may also prepare additional protocols and participate in the negotiation of future instruments and the further evolution of the Convention;
12. Parties to the Convention engage with each other in trusted and efficient cooperation which will benefit Small Island Developing States such as Fiji in terms of capacity building and international engagement;
13. increased cooperation by private sector entities with criminal justice authorities of Parties to the Convention given that Parties need to have a domestic legal framework on cybercrime and electronic evidence in place;
14. access to capacity building programmes; such technical assistance is necessary to facilitate full implementation of the Convention and to enhance the ability to cooperate internationally.
	1. Therefore, given that Fiji’s accession to the Convention will greatly contribute to the overall development of cyber security for Fiji and thereby assist in providing secure and reliable cyberspace for Fijians, it is essential to realise the benefits promised by globalised and digitised ICT infrastructure which include:
		* 1. the protection of personal data and the integrity of interconnected networks, which is critical for the overall prosperity, security and promotion of human rights and the support of broader economic and social development;
			2. enhancing the fight against cybercrime through continuous monitoring, analysing and managing cyber threats and risks, which ensures the safer use of cyberspace; and
			3. effective and efficient detection, investigation and prosecution of perpetrators of cyber related offences, both nationally and internationally.
15. **RECOMMENDATION**

5.1 It is recommended that Fiji ratifies the Convention without reservations.