Submission on New Zealand's written statement to the second session of the UN Cybercrime Treaty negotiations

I am law academic[1] and, on the whole, I support New Zealand's written statement to the second session of the United Nations (UN) Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes (UN Cybercrime Treaty). Overall, the proposed criminalisation provisions contained in the written statement are reasonable and well-founded based on established laws, procedures and practices concerning cybercrime. I do have the following comments and suggestions to specific parts of the written statement.

Consensus and acceptance

The country's position to strive for consensus and universal acceptance of a UN Cybercrime Treaty makes sense. Given than cybercrime is inherently multijurisdictional in nature as it is typically carried out across jurisdictions and affects many countries at the same time, a treaty that is acceptable to as many states as possible is a crucial goal. Short of this, the envisioned treaty will be a patchwork legal framework where cybercriminals can take refuge in safe havens where they can conduct their illegal activities or escape to with their criminal gains. To achieve greater consensus among states that have different political, social and cultural contexts, it is advisable to primarily focus on the criminalisation of core or "pure" cybercrimes such as illegal access, illegal interception, data interference, system interference, and misuse of devices.[2] These crimes are principally about cybersecurity or protecting the confidentiality, integrity and availability of computer data and systems.

Illegal access

The proposed text on illegal access is fine. It seems to be based on article 2 of the Budapest Convention on Cybercrime[3] and includes the portion on infringing security measures in the EU Cybercrime Directive.[4] I would suggest including the requirement of criminal intent in the commission of this crime and other core cybercrimes. The inclusion of criminal intent as an essential element will ensure that lawful, legitimate and commons activities such as information security research, cybersecurity testing, and ethical hacking are not covered under this crime and negatively impacted.[5] Further, the requirement of criminal intent (i.e., malice, dishonest intent, or intent to cause damage) can serve as a bar to the criminal prosecution of ordinary users for mere terms of service violations.[6] The suggested wording is:

---

[1] Michael Anthony C. Dizon, PhD, Senior Lecturer at Te Piringa Faculty of Law, University of Waikato.
[2] See Budapest Convention on Cybercrime, arts 2-6; see also EU Cybercrime Directive, arts 3-7.
[3] Budapest Convention on Cybercrime, art 2.
[4] EU Cybercrime Directive, art 3.
[5] See Michael Anthony C Dizon, *A Socio-Legal Study of Hacking: Breaking and Remaking Law and Technology* (Routledge 2018) 221-224; see also Electronic Frontier Foundation, "Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems" (8 February 2011) 5-8.
[6] See Marcia Hofman and Rainey Reitman, "Rebooting Computer Crime Law Part 1: No Prison Time For Violating Terms of Service" <https://www.eff.org/deeplinks/2013/01/rebooting-computer-crime-law-part-1-no-prison-time-for-violating-terms-of-service> accessed 18 May 2022; see also Michael Dizon, *A Socio-Legal Study of Hacking* 135.

"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 access to the whole or any part of a computer system without right A Party may require that the offence be committed by infringing security measures, with malice, intent to cause damage, the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

Illegal interception

The proposed provision on illegal interception is acceptable. It is should be noted though that New Zealand laws use the term "communication" rather than "transmissions", which is the more commonly used term in cybercrime laws.[7] The Crimes Act 1961, the Search and Surveillance Act 2012 and the Telecommunications (Interception Capability and Security) Act 2013 (TICSA) focus exclusively on communications.[8] However, communication is a much narrower term because it has historically been regulated under traditional telecommunications laws and is associated with wired or wireless communications. The problem is that with the technical and media convergence brought about by digitisation, the internet, and IP-based technologies, the concept of communication is no longer as relevant and has limitations. For instance, the transfer of a file from a computer to a cloud storage service such as Google Drive is more appropriately deemed a data transmission rather than a communication. Given that transmission as opposed to communication is the more precise term, the relevant New Zealand laws should be updated or interpreted accordingly.

I would also recommend the inclusion of a criminal intent requirement in this crime. The provision can read:

"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, malice, intent to cause damage, or in relation to a computer system that is connected to another computer system."

Cyber-extortion

With the increasing incidences of ransomware attacks, it is important to address this emerging form of cyberattack. Due the prevalence and sophistication of recent major attacks using ransomware, it could be argued that it has evolved into a distinct species of cybercrime that needs to be regulated. While certain aspects of ransomware are already covered by existing cybercrimes such as illegal access, data interference, and misuse of devices, the criminalisation of constitutive acts or elements involving ransomware should be considered. To prevent this proposed new cybercrime from being too broad and overlapping with other cybercrimes, the crux of the crime can be the negative impact or effects on the owner's possession, control or

[7] See Budapest Convention on Cybercrime, art 3; see also EU Cybercrime Directive, art 6.
[8] See Crimes Act 1961, ss 216A-216C; see also Search and Surveillance Act 2012, art 3(1) (e.g., definitions of computer systems, intercept, private communication); see also Telecommunications (Interception Capability and Security) Act 2013, art 3(1).

use of computer data and system. This is not directly or sufficiently covered by any existing cybercrimes.

Sexual exploitation of children using computer systems

The proposal to criminalise online sexual exploitation and abuse of children is in line with the Budapest Convention on Cybercrime, which has an article on offences against child pornography.[9] While the protection of children against sexual abuse and exploitation online is an important matter, it may be wiser to leave it to more specialised, existing laws such as the Lanzarote Convention and other international and national enactments concerning child protection.[10] Nonetheless, the proposed UN Cybercrime Treaty may contain provisions that refer to the criminal provisions in these other conventions and also confirm that the procedure rules in the Treaty apply to the investigation and prosecuting of crimes against children.

Posting or distributing an intimate visual recording without consent

While is a real and growing problem, revenge porn is better addressed under general criminal law or special laws that deal with this matter. It seems out of place in a cybercrime treaty because it does not directly or primarily concern or relate to information security or cybersecurity per se. It is worth noting that the crime of revenge porn is not provided for in the Budapest Convention on Cybercrime or EU Cybercrime Directive.

Crimes relating to infringement of copyright and related rights

It is appropriate that the written statement does not advocate for nor mention the inclusion of criminal provisions for offences relating to intellectual property rights violations. While there is a specific article in the Budapest Convention on Cybercrime about this,[11] matters relating to infringement of copyright or any other intellectual property right are best left to international and national intellectual property laws, which are well established and developed.[12]

Criminalisation of money laundering

It is true that there is already an existing international legal framework on money laundering. However, with advent and greater use of bitcoin, cryptocurrencies and other crypto assets as targets or proceeds of crimes, there are technical or computer-related elements in money laundering that can be specifically addressed in the context of cybercrime. For instance, the development, provision and use of cryptocurrency tumblers or mixers for money laundering has distinct technical dimensions that are more appropriately dealt with in cybercrime laws rather than general money laundering regulations. The same is true with the use of blockchain analysis for cybercrime investigations and evidence gathering. This is an area that requires further examination.

---

[9] Budapest Convention on Cybercrime, art 9.
[10] See COE Convention on Protection of Children Against Sexual Exploitation and Sexual Abuse; see also UN Convention of the Rights of the Child.
[11] Budapest Convention on Cybercrime, art 10.
[12] See Berne Convention; see also WIPO Internet Treaties.

Definitions

Access information is an important term in relation to cybercrime. New Zealand has a concise and useful definition of this term in the Search and Surveillance Act 2012. The country should put forward the inclusion of this definition in the proposed Treaty: "access information includes codes, passwords, and encryption keys, and any related information that enables access to a computer system or any other data storage device".[13]

[13] See Search and Surveillance Act 2012, art 3(1).