The discussion for an international standard of norms for the internet[Φ]

> …the Internet remains both a global commons and part of each nation's sovereign infrastructure, and thus activities in cyberspace must continue to navigate two sets of demands: national interests and global interests.[1]

1. Introduction

There is very little in our lives today that is not affected by the growth of the Interconnected Network, more popularly known as the Internet. The internet has given our personal and professional lives global reach. The internet is a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.[2]

Undoubtedly, the internet has changed the way we live our lives. Many services are now rendered 'electronically, including e-government, e-banking, e-health, and e-learning, next-generation power grids, and air traffic control'.[3] It is therefore imperative that these systems are protected against attack or from use that is harmful. The confidentiality, integrity and availability, the '"CIA' triad"[4] of the internet should be a matter of concern all over the world, because the crimes are being committed worldwide.

In 2000 the Love Bug virus designed by a programmer from the Philippines, one Onel de Guzman, shut down and destroyed computer systems in 45 countries.[5] Since 2003, Espionage was committed by China towards the United States at an unprecedented scale when hackers gathered nearly ten terrabytes of information from the Department of Defense in an operation known as Titan Rain.[6]

Φ Statement by Sakeus E.T. Shanghala, MP the Minister of Justice of the Republic of Namibia at the St Petersburg Legal Forum, May 16, 2019, Russian Federation.

1 Mellisa Hathaway, 'Connected Choices: How the Internet Is Challenging Sovereign Decisions', *American Foreign Policy Interests*, Vol. 36, No. 5, 2014 at p.309.

2 Defined on *Technopedia* available at <https://www.techopedia.com/definition/2419/internet> accessed 15 May 2019.

3 Hathaway (n 1) at p. 301. We have also heard of the Russian Minister of Justice refer to e-notorization.

4 Jim Waldo, Katherine Mansted, Benjamin Goh and Jiwon Ma, 'A Framework for Cybersecurity', Belfer Center, Harvard Kennedy School, 2018, p.1 accessed on May 16, 2019 at <https://www.belfercenter.org/sites/default/files/files/publication/FrameworkforCybersecurity.pdf>. CIA stands for **c**onfidentiality, **i**ntegrity and **a**vailability.

5 Susan W Brenner and Joseph J. Schwerha IV, 'Cybercrime Havens: Challenges and Solutions', *Business Law Today*, Vol. 17, No.2 (November/December 2007) American Bar Association, p.49.

6 Phillip Pool, 'War of the Cyber World: The Law of Cyber Warfare', *The International Lawyer*, Vol. 47, No. 2 (FALL 2013), American Bar Association at p.306.

With the 2014 attack on the Sony Pictures computer network, personal mails and the entire network of Sony Pictures was destroyed by North Korean hackers in retaliation for the release of an embarrassing satirical movie targeting their leader.[7] One can go on and on in reciting how crimes over the internet are causing havoc across the world.

When crimes are committed over the internet, using Information Communication Technology (ICT), or targeting ICT infrastructure, or when its users are the victims, or when others are victimized by conduct which weaponized the internet to cause harm in whatever form, the apt term *cybercrime* is used, yet hitherto, it has been elusive of an exact legal or forensic definition of the proscription of the crime, and to make matters worse, the term does not define or describe a clear category of criminal offences.[8]

This discussion hopefully exposes the need for norms at an international level to define terminologies, so that there is legal uniformity across the globe in relation to how acts committed over the internet will be handled in criminal justice systems. We will explore the arguments around the cyberspace discourse, and refer to examples and initiatives currently underway at some sort of regulation, and in reductionist fashion,[9] attempt to analyze them.

2. Legal Uniformity

If the *cyberspace* is to be regarded as the 'total inter-connectedness of human beings through computers and telecommunication without regard to physical geography'[10], then it is clear that like globalization, the internet (and harm over the internet) can and will affect everyone across any natural or political border. If the collection of data is unlawful in one country and not in the other, incongruities arise in criminalizing conduct, and when conduct from a source in one country affects others in another country, then conflict of laws may end up merely confusing the situation. Take the term *cyber espionage* or *cyber spying* as an example. When would it be committed?

Google and Apple and other technology companies store stashes of data. What offence would a hacker in Country A hacking those systems in Country B be committing? There is no certainty as to what is a *cyber attack* or act of *cyber war* under the general rubric of *cyber security*. It remains difficult to determine when an act of vandalism and damage to internet infrastructure (and systems running off of it) would amount to an act of war.

James A. Lewis in his paper on *Multilateral Agreements To Constrain Cyberconflict* offers this definition of cyber war:

---

[7] Waldo et al (n 4) at p.19.

[8] United Nations Office on Drugs and Crime, 'Comprehensive Study on Cybercrime' (2013) accessible at <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> last accessed on May 16, 2019, pp.11-12.

[9] Regrettably, this is not a colloquium on the subject matter. A full hour can be spent advancing this paper alone.

[10] Pool (f 6) at p.308).

> Agreement on what constitutes an act of war in cyberspace would be helpful. This could be defined as any action that produced an effect equivalent to an armed attack using kinetic weapons. One fundamental question is whether a cyberexploit must produce physical damage and casualties to be regarded as the use of force or whether intangible damage can be considered a use of force and an act of war.[11]

Microsoft agrees with Lewis, and have suggested the adoption of a Digital Geneva Convention.[12] This view did not go unnoticed by China, Kazakhstan, Kyrgystan, the Russian Federation, Tajikistan and Uzbekistan who jointly in a letter dated January 9, 2015 submitted a letter to the United Nations Secretary General suggesting an international code of conduct for information security, whist at the same time underlining the role that the United Nations can play in combating the criminal misuse of information technologies. To do nothing is not an option for the global community as we may render the 'cyberspace a lawless territory".[13]

3. Legislative Reforms

The next best thing beyond the touted code of conduct is the Convention on Cybercrime of the Council of Europe. Also known as the Budapest Convention on Cybercrime of 2001, it came into force on July 1, 2004 and with 57 states having ratified it, including non-Council of Europe states (such as the USA, Japan, Israel) makes it is by far the most widespread instrument. The African Union Convention on Cyber Security and Data Protection of 2014 is the second relevant instrument by numbers. However, China and Russia have not signed the Budapest Cybercrime Convention, and these two countries are important in the discourse just as they are in any geopolitical arena.

The African Union Convention on Cyber Security and Personal Data was the first attempt at creating a uniform form of protection of data on the internet on the continent. However, the Convention falls short in that it does not criminalize cybercrimes. Article 25 of the Convention states that:

> Each State Party shall adopt such legislative and or regulatory measures as it deems effective by considering as substantive criminal offences acts which affect the confidentially, integrity, availability and survival of information and communications technology systems, the data they process and the underlying network infrastructure, as well as effective procedural measures to pursue and prosecute offenders.[14]

---

[11] *Arms Control Today*, Vol. 40, No. 5 (JUNE 2010), published by Arms Control Association at p.16.
[12] Ciglic, K., 'Why we urgently need a Digital General Convention' (2017) *Observer Research Foundation* available at <https://www.microsoft.com/en-us/cybersecurity/blog-hub/why-we-urgently-need-digital-geneva-convention> accessed on August 20, 2018.
[13] ibid.
[14] African Union Convention on Cyber Security and Personal Data Protection, adopted by the 23rd ordinary session of the assembly held on 27 June 2017 at Malambo, Equatorial Guinea available at <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> last accessed on May 16, 2019.

Although no AU Member States have ratified the Convention, several have enacted or proposed domestic cyber security legislation.

Sections of South Africa's Protection of Personal Information Act, 2013 (Act No. 4 of 2013) went into effect shortly before the AU adopted its Convention. Kenya, Madagascar, Mauritania, Morocco, Tanzania, Tunisia, and Uganda are in the process of adopting national cyber security legislation. Commentators who have studied the text of those laws claim that these laws have potential human rights concerns, in that some of the proposed legislation seem to place extreme restrictions on the freedom of expression.[15]

The Budapest Convention is a criminal justice treaty with a specific focus on cybercrime and electronic evidence. It requires Parties (a) to criminalize a range of offences against and by means of computers, (b) to provide criminal justice authorities with procedural powers to secure electronic evidence in relation to any crime and (c) to engage in efficient international cooperation.

The AU Convention is, on the one hand, broader than the Budapest Convention in that it covers- electronic transactions; personal data protection; cyber security and cybercrime Thus, the AU Convention is an attempt to unite different aspects related to information technology law and certain non-digital and non-criminal justice issues. On the other hand, however, with regard to cybercrime and electronic evidence, the AU Convention criminalizes some but not all of the conduct foreseen under the Budapest Convention. Moreover, the AU Convention does not provide for the full set of procedural powers for investigating and prosecuting cybercrime and securing electronic evidence in domestic investigations. And finally, the AU Convention does not contain specific provisions and does not constitute a legal basis for international cooperation on cybercrime and electronic evidence. Overall, however, it would seem that though provisions and aspects are missing, those provisions that are available within the AU Convention – in spite of inconsistencies – are largely not in conflict with the Budapest Convention.[16]

I have already mentioned the foresight of the 4 members of the Shanghai Cooperation Organization[17] who have made proposals for a Draft International Code of Conduct for Information Security. Fusing all the convention texts and norms, this Code of Conduct and the direction it was steered could very well spark the beginning of debate to harmonize an international law response to all matters cyber.

---

[15] Mailyn Fidler & Fadzai Madzingira 'The African Union Cybersecurity Convention: A Missed Human Rights Opportunity' (*Council on Foreign Relations*, 2015) available at <https://www.cfr.org/blog/african-union-cybersecurity-convention-missed-human-rights-opportunity>.

[16] Zahid Jamil 'Comparative analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime' (*GLACY + Project*, 20 November 2016) available at <https://rm.coe.int/16806bf0f8>.

[17] For that and other efforts by the Shanghai Cooperation Organization, one can visit https://ccdcoe.org/organisations/sco/ last accessed on May 16, 2019.

4. Conclusion

For as long as efforts are not coordinated, countries that do not intend to be safe havens for cyber criminals will end up being such, even when they have promulgated laws at the national level, with legal definitions that are not congruent to the next country's definitions, with norms that differ and in an uncoordinated effort, they end up aiding the villains and less the law enforcers.

Hence the need for norms at an international level, just as there are now established norms and laws over the law of the sea or outer space. Only, we cannot just permit the passage of time to guide us to consensus. Too much is at stake with the internet. Bold leadership is required in not only setting the scene for a discussion on norms for the internet at an international level, it will also be required to extract consensus out of us if we are to defeat the criminal syndicates who are ever advanced ahead of law enforcement agencies generally.

End.

Reference (OSCOLA)

Brenner, S. and Schwerha IV, J.J. 'Cybercrime Havens: Challenges and Solutions' (2007) *Business Law Today* (Vol. 17, No. 2) pp. 48-51 available at <http://www.jstor.org/stable/23296752> accessed June 7, 2018.

Ciglic, K., 'Why we urgently need a Digital General Convention' (2017) Observer Research Foundation available at <https://www.microsoft.com/en-us/cybersecurity/blog-hub/why-we-urgently-need-digital-geneva-convention> accessed on August 20, 2018.

Hathaway, M. 'Connected Choices: How the Internet is challenging Sovereign Decisions' (2014) *American Foreign Policy Interests* (Vol. 36, Number 5).

Lewis. J., 'Multilateral Agreements To Constrain Cyberconflict' (2010) *Arms Control Today* (Vol. 40, No. 5) pp. 14-19 available at <http://www.jstor.org/stable/23628809> accessed June 6, 2018.

Pool, P., 'War of the Cyber World: The Law of Cyber Warfare' (2013) *The International Lawyer* (Vol. 47, No. 2) pp. 299-323 available at http://www.jstor.org/stable/43923953 at

United Nations General Assembly 'Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgystan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General' (2015) (A/69/723) New York.

United Nations Social Economic Council 'Guide for the thematic discussion on criminal justice responses to prevent and counter cybercrime in all its forms, including through the strengthening of cooperation at the national and international levels' (2018) (E/CN.15/2018/6) Vienna.

Waldo, J., Manstead, K., Goh, B., & Ma J. 'A Framework for Cybersecurity' [2018] Belfer Center, Harvard Kennedy School.