Defence Against Terrorism Review
Vol. 6, No. 1, Spring&Fall 2014, pp. 31-46

ISSN: 1307-9190

Deterring Cyberterrorism in the Global Information Society: A Case for the Collective Responsibility of States

Uchenna Jerome Orji
Research Associate at the African Centre for Cyber Law and Cybercrime Prevention (ACCP), Kampala, Uganda.
jeromuch@yahoo.com

Abstract: *The increasing interconnectivity of countries and national critical infrastructures in today's global network society have ushered the world into what has been aptly described as "an age of interdependence where each nation's security is also dependent on the actions of the other nations of the world." This state of affairs clearly underscores the need for the collective responsibility of states for global cybersecurity. This article explores some prospects towards enhancing the collective responsibility of states to deter cyberterrorism. It particularly suggests the need for a state to be held accountable where its failure to establish regulatory measures to deter or prosecute cybercrimes or cyberterrorism within its territory has allowed the perpetration of such acts and the causation of transboundary effects in other states.*

Keywords: *Cyberterrorism, information society, collective responsibility, legal framework, transboundary effects, attribution, critical information infrastructure*

Introduction

The emergence of the information society following the integration of computer and digital communications technologies into all aspects of life has redefined traditional notions of security. Malicious conduct against computer systems and networks now has the potential to affect individuals, countries and the global economy in ways previously unimagined. Consequently, one of the most

critical challenges of the information society has been the need to deter cyberterrorism. For the purposes of this article, cyberterrorism refers to terrorist attacks against computers and networked infrastructure which aim to hinder the operation of critical infrastructures and further terrorist objectives by causing the loss of lives, panic, widespread economic failure or intimidation in order to affect political conduct. This article examines the concept of cyberterrorism and suggests that the increasing interconnectivity of countries and national critical infrastructures in the global network society underscores the need for the collective responsibility of states for global cybersecurity, including the deterrence of cyberterrorism. Accordingly, this article proposes several strategies towards enhancing the collective responsibility of states to respond to cyberterrorism. This includes *inter alia* the need for every state to establish appropriate deterrent legal measures that would ensure that activities in cyberspace that are conducted within its jurisdiction do not cause transboundary harm in other states. It particularly suggests the need for a state to be held accountable where its failure to establish regulatory measures to deter or prosecute cybercrimes or cyberterrorism within its territory has allowed the perpetration of such acts and the causation of transboundary effects in other states.

Defining Cyberterrorism

'Cyberterrorism' is a term that is used to classify malicious activities that embody the twin elements of cybercrime and terrorism. According to Judge Stein Schjølberg,[2] "terrorism in cyberspace consists of both cybercrime and terrorism. Terrorist attacks in cyberspace are a category of cybercrime and a criminal misuse of information technologies. The term 'cyberterrorism' is often used to describe this phenomenon."[3] In a constricted sense, the term 'cyberterrorism' refers to the unlawful use of computers and networked communications infrastructure to carry out disruptive acts or attacks with the aim of hindering the operation of critical infrastructures[4] such as transport, energy and communications sectors or "threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in

---

[1] *See* Lt. Gen. Harry D. Raduege *(Ret.)* "Fighting Weapons of Mass Disruption: Why America Needs a 'Cyber Triad', in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway* (Andrew Nagorski, ed., East West Institute, 2010), p. 13.

[2] Judge Stein Schjølberg (Justice of the Court of Appeal, Norway) is the Chairman of the EastWest Institute Cybercrime Legal Working Group and also the Chairman of the International Telecommunication Union (ITU), High Level Expert Group (HLEG) on Cybersecurity that produced the ITU Global Security Agenda in 2008. Cybercrime Law, Biography of Stein Schjolberg, at http://www.cybercrimelaw.net/biography.html (accessed 14 October 2014).

[3] See Stein Schjølberg, *Terrorism in Cyberspace – Myth or reality?* (NATO Advanced Research Workshop on Cyberterrorism, Sofia, Bulgaria, October 2007), p. 3, available at http://www.cybercrimelaw.net/ documents/Cyberterroism.pdf (accessed 14 October 2014).

[4] "Critical infrastructures" refer to key infrastructures or sectors that are vital to the functioning of modern societies. What constitutes critical infrastructure varies in different countries, however, where the prolonged disruption of a sector or infrastructure would affect the well being of a nation by causing severe military and economic dislocation then such sector or infrastructure would qualify to be classified a "critical infrastructure." Sectors that are classified as critical infrastructure include (but are not limited to the following): banking and finance: government services: telecommunication/ information and communication technologies (ICTs); emergency/rescue services; energy/electricity; health services; transportation, logistics, distribution, and water (supply). *See* Uchenna J. Orji, *Cybersecurity Law and Regulation* (Wolf Legal Publishers, 2012), pp. 24-30.

furtherance of political or social objectives"[5] or other terrorist objectives. Thus, in this regard, the term cyberterrorism is used to define any act of terrorism that uses information systems or computer technology either as a weapon or as a target.

However, in a more generic sense 'cyberterrorism' may be used to broadly classify unlawful activities relating the terrorist use of the Internet, or threats or actual malicious acts carried out either by physical or virtual means against computers, networks, or critical infrastructures with the intention to cause harm or to coerce a government or its people in furtherance of social, ideological, religious, or political objectives. Here the term is used more broadly to refer to physical or virtual acts of terrorism that use computer information systems and also includes the terrorist use of networked information communications technologies to carry out activities such as spreading terrorist propaganda, propagating terrorist ideology, mobilizing recruits and supporters, gathering information, preparing for real world attacks and financing terrorist activities. While the above definitions are not comprehensive, there is currently no internationally accepted definition of 'cyberterrorism.' However, there has been an attempt to forge a legal definition of the term in the Draft Proposal for an International Convention on Cybercrime and Terrorism which was developed in 1999 as a proposal to globally address cybercrime following the conference on "International Cooperation to Combat Cybercrime and Terrorism" at the Stanford University in the United States.[6] The Draft Convention defines 'cyberterrorism' as the "intentional use or threat of use, without legally recognized authority, of violence, disruption or interference against cybersystems,[7] when it is likely that such use would result in death or injury of a person or persons, substantial damage to physical property, civil disorder, or significant economic harm."[8] However, other definitions of cyberterrorism appear not limit the target to only cybersystems but also includes any terrorist attack carried out through the Internet or against cyberinfrastructure.

Another legal definition of 'cyberterrorism' is found in the Black's Law Dictionary where it was defined as "terrorism committed by using a computer to make unlawful attacks and threats of attacks against computers, networks, and electronically stored information, and actually causing the target to fear or experience harm."[9] Although the above definitions may not be comprehensive, however, they maybe used to establish a minimum standard of what can be regarded as cyberterrorism.

---

5 *See* Dorothy Denning, "Cyber Terrorism" (Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, 23 May 2000). Regarding the definitions of cyberterrorism, see generally, Sarah Gordon and Richard Ford, *Cyberterrorism?* (Symantec Security Response, 2003).

6 *See* Abraham D. Sofaer, et al, *A Proposal for an International Convention on Cyber Crime and Terrorism,* unpublished, August 2000, available at http://www.iis-db.stanford.edu/pubs/11912/sofaergoodman.pdf (accessed 14 October 2014); *see* Abraham D. Sofaer, "Towards an International Convention on Cyber Crime" in *The Transnational Dimension of Cyber Crime and Terrorism* (Seymour E. Goodman, and Abraham D. Sofaer, eds., Hoover Institution Press, 2001), p. 225.

7 A "cyber system" is defined as "any computer or network of computers used to relay, transmit, coordinate or control communications of data or programs.". *See* Article 1(3), Draft International Convention on Cyber Crime and Terrorism in Sofaer,, *A Proposal for an International Convention on Cyber Crime and Terrorism,*

8 *See* Article 1(2) Draft International Convention on Cyber Crime and Terrorism. Ibid.

9 *Blacks Law Dictionary* (8th Edition, West Group, 2004), p. 1513.

The effect of a malicious act in cyberspace or the intent of a malicious actor in cyberspace may also be used to determine situations where an act of cyberterrorism has occurred. For example, the effect of a malicious act may be classified as cyberterrorism when such causes disruptive effects that are enough to generate fear comparable to a traditional act of terrorism, even if such acts were done by mere criminals.[10] In determining whether the effects of an attack qualify as cyberterrorism, Professor Denning notes that:

> To qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[11]

On the other hand, the intent of a malicious actor may be used to classify an act as cyberterrorism where for example unlawful attacks are carried out against computer systems with the aim of hindering the operation of critical infrastructures to achieve objectives such as intimidating or coercing a government or people or to further a social, political or religious objective, or to cause grave harm or severe economic damage in a society.[12] For example, if a criminal hacks into a bank customer's account and steals credit card information, such activity may be referred to as mere cybercrime, because the intent of the criminal actor is neither political nor social. However, if similar attacks are directed to a substantial number of bank accounts and the responsible criminal actor declares that he/she is going to continue attacks until the government accepts his demands then such conduct is labeled as cyberterrorism.[13] As such, once there is a terrorist intent common acts of cybercrime may constitute cyberterrorism. Such acts include hacking, virus dissemination, website defacing, denial-of-service (DoS) attacks, disrupting critical information infrastructures, and issuing threats to disrupt computer-based infrastructure either by virtual or physical means.

Exploring Prospects to Enhance the Collective Responsibility of States to Deter Cyberterrorism

Responding to cyberterrorism has been a challenging issue. Due to the universal nature of information networks, virtual terrorist attacks can be launched from anywhere in the world. Tracing the origin of such terrorist attacks in cyberspace is usually a huge challenge, assuming the attacks are even detected at all. This is because of the ability of terrorists to use anonymous communication

---

[10] John Rollins and Clay Wilson, "Terrorist Capabilities for Cyber Attack: Overview and Policy Issues," (RK 33123, CRS Report for Congress, January 22, 2007), p. 3, available at http://fas.org/sgp/crs/terror/ RL33123.pdf (accessed 8 December 2014).

[11] *See* Denning, *Cyber Terrorism*.

[12] *See* Rollins and Wilson, "Terrorist Capabilities for Cyber Attack: Overview and Policy Issues."

[13] *See* Murat Dogrul, Adil Aslan, and Eyyup Celik, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism," in *Proceedings of the 3rd International Conference on Cyber Conflict* (NATO/CCD COE Publications, 2011, pp. 31-32, available at http://www.ccdcoe.org/publications/2011proceedings/Developing AnInternationalCooperation...-M.%20Dogrul-Aslan-Celik.pdf (accessed 14 October 2014).

facilities and encryption technology to hide their identity, as well as loop attacks through computer systems in various countries that may not have cybercrime laws[14] and other deterrence mechanisms. Thus, terrorist actors may originate or transmit cyberattacks from jurisdictions where legal mechanisms and other cybersecurity measures are either weak, not yet in existence or from permissive jurisdictions that appear to provide safe havens for such conduct by not prosecuting such actors or permitting their extradition. Hence, countries that do not have cybercrime laws apparently create safe havens for cyberterrorist activities. This is because in countries where malicious cyberactivities have not been criminalized, any related conduct by malicious actors may not be successfully prosecuted on the basis of the principle of *nullum crimen nulla poena sine lege*.[15] This principle implies that a person shall not be convicted of a criminal offence unless that offence is defined and the penalty is prescribed in a written law.[16]

However, with the growing application of information technologies in all aspects of life and the increasing interconnectivity of national critical infrastructures and global information networks, all states are now exposed to the threats and vulnerabilities, such as cyberterrorism, that affect an information society. Consequently, effective solutions to address these threats and vulnerabilities will require the active cooperation of all state actors in the global information society. A major step towards addressing this challenge is for all states to establish cybercrime laws that prohibit terrorist conduct in the information society. Every state is a stakeholder in the global information society; hence, it follows that every state has a duty to take reasonable and appropriate measures towards securing this society by ensuring that cyberactivities within its jurisdiction do not cause transboundary harm in other states. This underscores the collective responsibility of states for global cybersecurity. This concept is already entrenched in Article 5A of the International Telecommunication Regulations which provides that:

> Member States shall individually and collectively endeavour to ensure the security and robustness of international telecommunication networks in order to achieve effective use thereof and avoidance of technical harm thereto, as well as the harmonious development of international telecommunication services offered to the public.[17]

Member states of the International Telecommunication Union (ITU) are also under an obligation to implement its regulations in a manner that respects and upholds their human rights obligations.[18] One way of implementing the regulations is through the establishment of legal measures to ensure the security and robustness of international telecommunication networks. Thus, within this concept of collective responsibility, there is an implied primary duty on every state to establish regulatory

---

[14] *See* Marco Gercke, *Understanding Cybercrime: A Guide for Developing Countries* (ITU, 2009), pp. 51-57.

[15] Latin for 'no crime or punishment without a law,' a basic principle of criminal law

[16] *Blacks Law Dictionary*, p. 1098.

[17] *See* Final Acts of the World Conference on International Telecommunications, *International Telecommunication Regulations*, (International Telecommunication Union, 2012); *see also* Article 45(1) of the Constitution of the International Telecommunication Union, available at http://www.itu.int/ en/history/Pages/ConstitutionAndConvention.aspx (accessed 25 November 2014).

[18] *See* Article 1, Constitution of the International Telecommunication Union. Ibid.

frameworks designed to provide an effective deterrent system and crossborder cooperation against cyberterrorist conduct that may affect the security and robustness of international telecommunication networks or cause transboundary harm. A state's failure to fulfill such duty should give rise to liability, since states have been held responsible where activities within their territories produced harmful transboundary effects in other countries. For example, in the *Trail Smelter Arbitration* that arose from a transboundary air pollution dispute between the United States and Canada, where damage had been caused to property in the United States due to air pollution which had originated in Canada, the arbitral tribunal held that "no State has a right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein, when the case is of serious consequence and the injury is established by clear and convincing evidence."[19]

The decision of the arbitral tribunal laid the foundation in establishing the principle that a state shall not "permit the use of its territory in such a manner as to cause injury in or to the territory of another."[20] This principle has now been enshrined in some aspects of international environmental and human rights law. Thus, "international law already requires states to control activities that may cause transboundary harm."[21] Consequently, states can be held responsible where activities within their territories produce harmful transboundary effects in other countries. In *Cyprus v. Turkey*,[22] the European Courts of Human Rights held that the responsibility of states can arise as a result of acts and omissions of their authorities which produce effects outside their own territory.[23] Accordingly, Professor Alan Boyle has also argued that:

> …human rights law could in appropriate circumstances have extra-territorial application if a state's failure to control activities within its territory affects life, health, private life or property in neighboring countries. If states are responsible for their failure to control soldiers and judges abroad, *a fortiori* they should likewise be held responsible for a failure to control transboundary pollution and environmental harm emanating from industrial activities inside their own territory.[24]

---

[19] *See* "The Trail Smelter Arbitral Decision", *American Journal of International Law* 35 (1941), p. 684.

[20] *See* Cesare P.R. Romano, *The Peaceful Settlement of International Environmental Disputes: A Pragmatic Approach* (Kluwer Law International, 2000), p. 261.

[21] *See* Principle 2, Rio Declaration on the Environment and Development, U.N.Doc.A/CONF.151/ 5/REV.1,31.I.L.M.874 (1992); Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports (1996) 226, at para 29; Articles on Trans-boundary Harm, ILC Report (2001) GAOR A/56/10, 366; *Tatar v. Romania* [2009] ECHR, para 111; *Osman v. the United Kingdom*, judgment of 28 October 1998, Reports 1998-VIII, p. 3164; *Calvelli and Ciglio v. Italy* [GC], no. 32967/96, ECHR 2002-IX, and *August v. the United Kingdom*, no. 36505/02, 21 January 2003; Alan Boyle, "Human Rights and the Environment: A Reassessment" (UNEP Paper Revised, 2010), p. 27; Thomas Gehring and Markus Jachtenfuchs, "Liability for Trans-boundary Environmental Damage Towards a General Liability Regime?" *European Journal of International Law* 4 (1993), pp. 92-106.

[22] [2001] ECHR No.25781/94; Alan Boyle, "Human Rights and the Environment: A Reassessment," *Fordham Environmental Law Review* 18 (2008), pp. 471-511; Boyle, "Human Rights and the Environment: A Reassessment," p. 26.

[23] *Ibid.*

[24] Ibid, p. 27.

To some extent, the norm that states may be held responsible for acts and omissions within their territories which produce transboundary harm in other countries may be applied for the purpose of promoting the concept of the collective responsibility of states for global cybersecurity.[25] Thus, where a state's failure to promote cybersecurity by establishing appropriate regulatory mechanisms to deter malicious cyberconduct has given rise to the existence of a safe haven for cybercriminality, that state should be held responsible for any transboundary harm that arises from the perpetration of cybercrimes in that safe haven. This implies that a state should be held responsible where its failure to establish adequate cybercrime laws and other deterrent regulatory measures within its territory has encouraged the perpetration and non-prosecution of cybercrimes that affected other states or individuals or organizations located in other states. The case of the "I LOVE YOU" Virus provides an example in this regard. The virus was created in 2000 by Onel de Guzman (a Filipino computing student at the AMA Computer University in Manila, Philippines) and spread worldwide through the Internet - infecting over 45 million computers and causing businesses billions of dollars in losses. Many of the affected businesses were located in the United States which had already established laws prohibiting cybercrime. When FBI agents succeeded in identifying the creator of the virus in Philippines, it was also found that the country did not have cybercrime laws under which he could be prosecuted. Philippines had an extradition treaty with the United States. However, there was no basis to apply for Onel de Guzman's extradition under the treaty, since Philippines had not criminalized the creation and spreading of computer viruses at that time.[26] Consequently, he was able to escape criminal liability for the enormous damage caused by the spread of the "I LOVE YOU" virus.[27] However, within the concept of the international norm that states may be held responsible for acts and omissions within their territories which produce transboundary harm in other countries, there are prospects that Philippines could have been held responsible for the transboundary effects of the "I LOVE YOU" virus, since the country failed to establish regulatory measures that might deter such cybercrimes or enable its prosecution. Thus, if a state can be held responsible for failure to control territorial activities that may cause transboundary harm, then there is a prospect that a state may also be held accountable where the failure to establish regulatory measures to deter or prosecute cybercrimes within it territories has allowed the perpetration of cybercrimes or acts of cyberterrorism that caused transboundary effects in other states.

Another step that would enhance the collective responsibility of states to deter cyberterrorism is the establishment of a single international treaty of all nations on cybersecurity. Thus, considering the ubiquitous nature of the information society and the transnational nature of cyberterrorism, a safe haven for cyberterrorism can only be eliminated if all states have access to one enforceable

---

[25] *See generally*, "*A Conceptual Approach for Setting a Standard of Care for cCross-border Internet* (Discussion paper of the Council of Europe Ad Hoc Advisory Group on Cross-border Internet for Workshop 6: Sovereignty of States and the Role and Obligations of Governments in the Global Multi-stakeholder Internet Environment, European Dialogue on Internet Governance (EuroDIG), Madrid, 28-29 April 2010),

[26] Following the incident, Government of the Philippines introduced the Electronic Commerce Act of 2000 (RA 8792) to criminalize the dissemination of computer viruses and other cybercrimes. Gilbert C. Sosa, "Country Report on Cybercrime: The Philippines" (UNAFEI, 140th International Training Course Participants' Papers, undated), p. 80.

[27] See Shannon C. Sprinkel, "Global Internet Regulation: The Residual Effects of the 'I LOVEYOU' Computer Virus and the Draft Convention on Cyber-Crime", *Suffolk Transnational Law Review* 25, (2002), pp. 492-493.

global cybersecurity treaty that defines and prohibits cybercrimes, including cyberterrorism, also creates a framework for mutual assistance amongst state parties. The adoption and ratification of such a global treaty by states will technically eliminate safe havens for perpetrators, since every state will have an obligation to deter, prosecute or assist other states in tackling cybercrimes and cyberterrorism. Thus, in order to ensure effective collective responsibility of states to deter cyberterrorism, it is imperative that such global treaty imposes obligations on states to establish legal measures to deter cyberterrorist activities and also enhance effective cross-border cooperation for the prevention or investigation and prosecution of such activities. Consequently, if potential perpetrators of cyberterrorism are aware that they cannot hide in any country in the world, they may to some extent be discouraged from committing such acts. However, the absence of such an international treaty has been an obstacle to the global harmonization of cybersecurity laws. This has also hindered the effective promotion of the concept of the collective responsibility states for global cybersecurity. Thus, the establishment of a global treaty on cybersecurity is imperative to secure the harmonization of cybersecurity laws amongst all sovereign states. Accordingly, a global treaty on cybersecurity would enhance a better understanding of cyberterrorism and other aspects of cybersecurity, and facilitate the development and deployment of measures that can help to increase resilience to the impacts of cyber threats.[28] Such a treaty would provide the minimum standards for the criminalization of cyberterrorism and serve as the basis for the global harmonization of related national laws. This has a great prospect of encouraging international cooperation to the widest extent possible amongst state parties for the purposes of investigations or legal proceedings concerning cyberterrorism.

The concept of a harmonized legal environment where all sovereign states can have access to one global treaty calls for the negotiation of an international cybersecurity treaty under the aegis of the United Nations General Assembly. Accordingly, Judge Stein Schjølberg argues that:

> Cyberdeterrence may best be achieved within a global framework of a United Nations Cyberspace Treaty on cybersecurity and cybercrime. Regional and bilateral conventions or treaties will not be sufficient. International law should provide the framework for peace and security in cyberspace.[29]

The United Nations has been working toward developing initiatives for an international treaty on cybersecurity;[30] however; there has also been a lack of consensus amongst states on what the focus of a cybersecurity treaty should be. For example, while Russia highly favors a cybersecurity treaty to regulate cyberwar or information warfare,[31] on the other hand the United States highly

---

[28] *See* Solange Ghernaouti-Hélie, "Need for a United Nations Cyberspace Treaty," (*WISIS Forum 2010-High-Level Debate on Cybersecurity and Cyberspace* (ITU, Geneva, 10-14 May, 2010), p. 1.

[29] Ibid, p. 13. *See also* Solange Ghernaouti-Hélie, "Need for a United Nations Cyberspace Treaty," p. 2. (where Professor Ghernaouti-Hélie made similar arguments).

[30] Orji, *Cybersecurity Law and Regulation*, pp. 96-112.

[31] Ibid, pp. 204-207; Dmitry I. Grigoriev, "Russian Priorities and Steps Towards Cybersecurity", in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway*, pp. 6-8; Dorothy Denning, "Obstacles and Options for Cyber Arms Controls," *Arms Control in Cyberspace* (Heinrich Böll Foundation, Berlin, Germany, June 29-30, 2001), pp. 4-5.

favors the criminalization of malicious conducts against computer systems by individual actors[32] as well as international cooperation to improve mutual legal assistance and extradition.[33] Also while states like China filter and prohibit certain information that may harm or damage the stability of state power as a part of their cybersecurity program,[34] other states like the United States see such activities as an impediment to free speech.[35] However, the United Nations has also been working toward developing initiatives to improve consensus on cybersecurity. In July 2010, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (a group of cybersecurity specialists and diplomats representing 15 countries which was established in 2009 pursuant to the United Nations General Assembly Resolution 60/45)[36] agreed on a set of recommendations for negotiations on an international computer security treaty which were transmitted to the United Nations Secretary General.[37] The Group of Experts Report noted *inter alia* the need for further dialogue amongst states to discuss norms pertaining to state use of ICTs to reduce collective risk and protect critical national and international infrastructure; the need for information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices; and the need for states to find possibilities to develop common terms and definitions relating to cybersecurity.[38]

Aside from the United Nations, some other international organizations have also developed initiatives to improve consensus on cybersecurity. An example is the Council of Europe, which developed the Council of Europe Convention on Cybercrime.[39] The Convention which currently has about forty-three state parties[40] is recognized as the only international treaty on cybercrime. It criminalizes four different categories of substantive offences in its Articles 2-10:

(1) offences against the confidentiality, integrity and availability of computer data and systems;

(2) computer-related offences;

(3) content-related offences and;

(4) offences related to infringements of copyright and related rights.

---

[32] Office of the President of the United States of America, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (The White House, Washington D.C., May 2011), p. 10; Paul Cornish, et al, *On Cyber Warfare* (The Royal Institute of International Affairs, Chatham House, 2010), p. 23.

[33] Office of General Counsel, *An Assessment of International Legal Issues in Information Operations* (U.S. Department of Defense, May 1999), p. 47.

[34] Uchenna J. Orji, "An Analysis of China's Regulatory Response to Cybersecurity", *Computer and Telecommunications Law Review* 7 (2012), pp. 212-226.

[35] Office of the President of the United States of America, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, pp. 5 and 10; Tang Lan and Zhang Xin, "Can Cyber Deterrence Work?" in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway*, p. 2.

[36] *See* United Nations General Assembly Resolution 60/45, para 4.

[37] See United Nations General Assembly, *Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Document A/65/201 (30 July 2010).

[38] Pauline C. Reich, et al, "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity," *European Journal of Law and Technology* 1(2) (2010), pp. 9-11.

[39] *See* the Council of Europe, Convention on Cybercrime, 41 I.L.M. 282 (Budapest, 23.XI, 2001).

[40] A list of state parties to the Convention is available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG (accessed 14 October 2014).

The above offences have been used by the Convention's state parties and several other states to establish a minimum standard of what can be regarded as cybercrime or computer crime.[41] As such the above offences can be regarded as establishing the consensus of the Convention's state parties on what constitutes a cybercrime since state parties have an obligation to ensure the criminalization of those offences in their municipal laws.[42]

Another example of consensus building on cybersecurity is the bilateral cooperation of experts from Russia and the United States under the auspices of the EastWest Institute[43] which produced twenty consensus terms on cybersecurity and information security. The terms are meant to serve as a conceptual framework to facilitate the challenging process of creating definitions for a common international lexicon on cybersecurity and information security. The effort is also intended to establish a foundation for international agreements or "rules of the road" on cyberspace and information security.[44] There has also been a similar bilateral cybersecurity initiative between experts from the United States and China under the auspices of the EastWest Institute.[45] Apparently, these developments indicate that there are prospects that the negotiation process for the development of a global cybersecurity treaty will enhance the development of a common standard for the criminalization of malicious cyberconduct, such as cyberterrorism and also facilitate the development of effective platforms for cross-border legal cooperation in that regard.

It is also imperative to enhance global research efforts towards the creation of an international system for the accurate attribution of any cyberattack or hostile action in cyberspace.[46] Accordingly, the Center for Strategic and International Studies (CSIS) report on cybersecurity aptly emphasizes that, "creating the ability to know reliably what person or device is sending a particular data stream in cyberspace must be part of an effective cybersecurity strategy."[47] Presently, the challenges of accurately attributing cyberattacks to a particular entity affects the categorization of cyberattacks as acts of terrorism or acts of war. For example, various incidents of cyberattacks in several countries such as Estonia and the United States have been categorized as acts of cyberwarfare and cyberterrorism in the media and speculatively linked to Russia[48] and China,[49] however given

---

41 *See* Stein Schjølberg, "The History of Global Harmonization on Cybercrime Legislation - the Road to Geneva" (unpublished, 2008), pp. 8-9, available at http://www.cybercrimelaw.net/documents/cybercrime _history.pdf (accessed 14 October 2014).

42 *See* ITU High Level Experts Group (HLEG), "ITU Global Cyber-Security Agenda (GCA)," *High Level Experts Group [HLEG] Global Strategic Report* (ITU, 2008), p. 16; Orji, *Cybersecurity Law and Regulation*, p. 119.

43 Further information about the activities of the EastWest Institute with respect to the development cybersecurity initiatives is available at EastWest Institute, "Cyberspace," at http://www.ewi.info/issues/cyberspace (accessed 14 October 2014).

44 *See generally*, Karl Frederick Rauscher and Valery Yaschenko, *Russia-U.S. Bilateral on Cybersecurity- Critical Terminology Foundations* (EastWest Institute and the Information Security Institute of Moscow State University, 2011).

45 *See* Karl Frederick Rauscher and Zhou Yonglin, *China-U.S. Bilateral on Cybersecurity: Fighting Spam to Build Trust* (EastWest Institute, 2011).

46 *See* Dmitry I. Grigoriev, "Russian Priorities and Steps Towards Cybersecurity," in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway*, p. 6.

47 *See* James A. Lewis, et al., *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th* Presidency (Center for Strategic and International Studies, December 2008), p. 62.

48 *See* Paul Meller, "Cyberwar: Russia vs Estonia", *Networkworld.com* (May 24, 2007) available at http://www.network-world.com/news/2007/052207-ec-urges-coordinated-effort-against.html (accessed 14 January 2012).

49 *See* Susan Landau, "National Security on the Line," *Journal of Telecommunications and High Technology Law* (2006), p. 429; *see generally* Micah Schwalb, "Exploit Derivatives and National Security," *Yale Journal of Law and Technology* 9 (2007), p. 162.

that these attacks were not traced with certainty to state or terrorist organizations, it becomes difficult to clearly categorize those incidents as cyberwarfare or acts of cyberterrorism. This has given rise to a state of mutual distrust which has been detrimental to international relations and prompting several accusations, denials and counteraccusations of state-sponsored cyberattacks between countries such as United States and China,[50] as well as Estonia and Russia. Thus, the problem of attribution presents the advantage of anonymity to terrorists since they can loop through different computer systems in the process of perpetrating cyberattacks or even orchestrate attacks to appear to originate from government computers in another country. Consequently, terrorists can employ cyberattacks to strike at the heart of society or infrastructure from a remote location or an unidentifiable address.[51] However, it has been shown that the establishment of trusted identification systems in Public Key Infrastructure (PKI) can help address the problem of attribution. For example, it is noted that the frequency of unauthorized intrusions into the United States Department of Defense (DOD) network decreased by 50 percent following the DOD's introduction of a new identification system (Common Access Card) to address authentication in 2008.[52] While this solution may not be possible on a global scale, it underscores the fact that the development of authentication mechanisms for digital identities will enhance attribution in cyberspace.

To address the challenge of attribution, it has also been aptly suggested that states such as Russia and the United States should champion the idea of establishing a binding multilateral agreement on Public Key Infrastructure (PKI) to promote internationally an "ecosystem" of trusted identities under the auspices of the International Telecommunication Union (ITU).[53] However, while such an arrangement is yet to come to life, there are prospects that the development of common ITU standards for the verification of networked digital devices would enhance attribution in cyberspace. Apparently, such mechanisms may raise concerns over anonymity in cyberspace, as well as fears of censorship and the infringement of the human rights to the freedom of expression and privacy by governments. This however underscores the need for an appropriate balance between Internet freedom/human rights and cybersecurity measures.

There is also need to enhance the capabilities of multilateral systems for early warning and cyberincident management. This will entail the strengthening of information sharing capacities of multilateral institutions such as the International Multilateral Partnership against Cyber Threats (IMPACT),[54] the NATO Cooperative Cyber Defense Centre of

---

[50] *See* Elizabeth M. Lynch, "Adam Segal Discusses U.S.-China Relations in a Cyber World," *China Law & Policy*, (April 14, 2010), available at http://chinalawandpolicy.com/2010/04/14/adam-segal-discusses-u-s-china-relations-in-a-cyber-world/. (accessed 14 January 2012).

[51] Paul Cornish, et al, *On Cyber Warfare* (The Royal Institute of International Affairs, Chatham House: London, 2010) p. 11.

[52] *See* Lewis, *Securing Cyberspace for the 44th Presidency*.

[53] Franz-Stefan Gady and Greg Austin, *Russia, The United States, and Cyber Diplomacy: Opening the Doors* (EastWest Institute, 2010), p. ii.

[54] The IMPACT operates a comprehensive Global Response Centre (GRC) which is designed to be the foremost cyber threat resource centre in the world. It aims to provide the global community with a real-time aggregated early warning system and assist member countries in the early identification of cyber-threats and also provides guidance on the necessary remedial measures. Through is way, the IMPACT plays a pivotal role in the realization of the ITU's Global Cybersecurity Agenda (GCA) objective of establishing technical measures to combat new and evolving cyber threats. *See* The International Multilateral Partnership Against Cyber Threats (IMPACT), at http://www.impact-alliance.org/ (accessed 14 October 2014).

Excellence[55] and the 24/7 Network of Contacts under the Council of Europe Convention on Cybercrime.[56] Apparently, many countries find it difficult to share critical cybersecurity information due to domestic sensitivities associated with national security. However, strengthening the capacities of these institutions on the basis of common interests or collective security in order to enhance the ability of their member states to share information, resources, and best practices on cybersecurity will go a long way towards facilitating timely warnings and responses to transnational cyberincidents such as cyberterrorism. This approach will require states to harmonize their cybersecurity and countercyberterrorism interests within the framework of multilateral institutions such as the IMPACT, the NATO Cooperative Cyber Defense Centre of Excellence and the 24/7 Network of Contacts and also share resources and best practices to facilitate their collective interests.

To further enhance the concept of the collective responsibility of states to promote global cybersecurity and deter cyberterrorism, it may also be necessary to develop international mechanisms for blacklisting states that do not develop standard regulatory measures to deter cybercrimes. A similar approach has been applied by the Financial Action Task Force (FATF) in fighting global money laundering.[57] Also, despite the absence of efficient attribution mechanisms, the development of a multilateral platform that is similar to the FATF may to some extent facilitate the prevention of some forms of cyberterrorism such as DoS attacks. This will require member states to agree to impose obligations on Internet Service Providers to scan the data traffic going to and from computers attached to their networks for unusual patterns of traffic that indicate botnet (zombie)[58] activity, and disconnect the associated computers.[59]

---

[55] The NATO Cooperative Cyber Defense Centre of Excellence is responsible for conducting research and training in cyber defense. In accordance with NATO collective security agenda, the major objective of the cyber defense centre is to help member states achieve collective self defense in the cyberspace by defying and countering threats of cyber warfare.

[56] *See* Article 35, Council of Europe Convention on Cybercrime. The establishment of the 24/7 network is hinged on the need to ensure a "round the clock" efficiency of mutual assistance requests and also to enhance the efficiency and speed of international cybercrime investigations. The Convention provides that each State 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 electronic evidence regarding a criminal offence under the Convention. Presently, countries that have not signed or ratified the Convention can join in the 24/7 network of contacts. *See* Report of the Second Meeting of the Cybercrime Committee T-CY (2007) 03 p. 3, cited in Gercke, *Understanding Cybercrime: A Guide for Developing Countries*, p. 215.

[57] *See* Financial Action Task Force (FATF), "High Risk and Non-Cooperative Jurisdictions," available at http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236992_1_1_1_1_1,00.html (accessed 14 October 2014).

[58] "Botnet" is a short term for a group of compromised computers running programmes that are under external control (also known as "zombie armies" or "drone armies"). Botnets may comprise networks of coordinated groups of several tens, hundreds or even thousands of computing devices such as PCs, laptops and even the new generation of mobile devices such as "smart phones" all infected with the same virus or other malware and compromised to turn them into "zombies" or "robots." Such computers can be controlled without the owner's knowledge. Criminals use the collective computing power and connected bandwidth of these externally-controlled networks for malicious purposes and criminal activities such as launching of Distributed Denial of Service (DDoS) attacks. *See* ITU (ICT Applications and Cybersecurity Division Policies and Strategies Department-ITU Telecommunications Development Sector) *Botnet Mitigation Toolkit* (ITU, 2008, pp. 1 and 5; *see also* Alana Maurushat, "Zombie Botnets", *SCRIPTed,* 7(2) (August 2010), pp. 371-383.

[59] *See* Lillian Edwards, "The Internet and Security: Do We Need a Man with a Red Flag Walking in Front of Every Computer," *SCRIPT-ed* 4(1) (March 2007), p. 1.

Conclusion

With the increasing interconnectivity of countries and national critical infrastructures in the global network society, the world has leaped into an age that has been aptly described as "an age of interdependence where each nation's security and prosperity is increasingly dependent on the actions of the other nations of the world."[60] This state of affairs underscores the need for the collective responsibility of states for global cybersecurity including the deterrence of cyberterrorism. States that fail to establish appropriate cybercrime laws would create safe havens for cybercrimes that would include cyberterrorism. Under international law, states are already under an obligation to "prevent and suppress in their territories through all lawful means the preparation and financing of any acts of terrorism."[61] Lawful measures to prevent and suppress the preparation and financing of terrorism include the establishment and harmonization of legal mechanisms to deter cyberterrorism and also enhance effective cross-border cooperation for the prevention or investigation and prosecution of such conduct. Thus, despite varying levels of digital development and economic disparity amongst states, a major step toward realizing the concept of the collective responsibility of all states to deter cyberterrorism should commence with the establishment of national regulatory mechanisms that eliminate safe havens for cybercrime as well as well as the facilitation of international cooperation to the widest possible extent.

BIBLIOGRAPHY

Boyle, Alan, "Human Rights and the Environment: A Reassessment" (UNEP Paper Revised, 2010).

Boyle, Alan, "Human Rights and the Environment: A Reassessment", *Fordham Environmental Law Review* 18 (2008).

Cornish, Paul, et al, *On Cyber Warfare* (The Royal Institute of International Affairs, Chatham House, 2010).

Denning, Dorothy, "Cyber Terrorism" (Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, 23 May 2000).

Denning, Dorothy, "Obstacles and Options for Cyber Arms Controls", *Arms Control in Cyberspace* (Heinrich Böll Foundation, Berlin, Germany, June 29-30, 2001).

Dogrul, Murat, Aslan, Adil, and Celik, Eyyup, "Developing an International Cooperation on Cyber

[60] Harry D. Raduege, "Fighting Weapons of Mass Disruption: Why America Needs a 'Cyber Triad', in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway*, p.13.

[61] *See United Nations Security Council Resolution 1373* (September 28, 2001); the *United Nations Security Council Resolution 1269* (October 19, 1999); the *International Convention for the Suppression of the Financing of Terrorism*, adopted by the General Assembly of the United Nations in Resolution 54/109 (9 December 1999); Article 4 of the African Union Convention on The Prevention and Combating of Terrorism (1994); and the United Nations Global Counter-Terrorism Strategy (2006).

Defense and Deterrence against Cyber Terrorism", in *Proceedings of the 3rd International Conference on Cyber Conflict* (NATO/CCD COE Publications, 2011).

Edwards, Lillian, "The Internet and Security: Do We Need a Man with a Red Flag Walking in Front of Every Computer", *SCRIPT-ed* 4(1) (March 2007).

Gady, Franz-Stefan and Austin, Greg, "Russia, The United States, And Cyber Diplomacy: Opening the Doors" (EastWest Institute, 2010).

Gehring, Thomas and Jachtenfuchs, Markus, "Liability for Trans-boundary Environmental Damage Towards a General Liability Regime?" *European Journal of International Law* 4 (1993).

Gercke, Marco, *Understanding Cybercrime: A Guide for Developing Countries* (ITU: Geneva, 2009).

Gordon, Sarah, and Ford, Richard, "Cyberterrorism?" (Symantec Security Response, 2003).

Grigoriev, Dmitry I., "Russian Priorities and Steps Towards Cybersecurity" in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway* (Andrew Nagorski, ed., East West Institute, 2010).

Ghernaouti-Hélie, Solange, "Need for a United Nations Cyberspace Treaty", *WISIS Forum 2010-High-Level Debate on Cybersecurity and Cyberspace* (ITU, Geneva, 10-14 May 2010).

ITU High Level Experts Group (HLEG), "ITU Global Cyber-Security Agenda (GCA)", *High Level Experts Group [HLEG] Global Strategic Report* (ITU, 2008).

ITU, *Botnet Mitigation Toolkit* (ITU, 2008).

Lan, Tang and Xin, Zhang, "Can Cyber Deterrence Work?" in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway* (Andrew Nagorski, ed., East West Institute, 2010).

Landau, Susan, "National Security on the Line" *Journal of Telecommunications and High Technology Law* 4 (2006).

Lewis, James A., et al., "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency" (Center for Strategic and International Studies, December 2008).

Lt. Gen. Raduege, Harry D. *(Ret.)* "Fighting Weapons of Mass Disruption: Why America Needs a "Cyber Triad", in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway* (Andrew Nagorski, ed.i East West Institute, 2010).

Lynch, Elizabeth M. "Adam Segal Discusses U.S.-China Relations in a Cyber World", *China Law & Policy* (April 14, 2010).

Maurushat, Alana, "Zombie Botnets", *SCRIPTed* 7(2) (2010).

Meller, Paul, "Cyberwar: Russia vs Estonia", *Networkworld.com* (May 24, 2007).

Office of the President of the United States of America, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (The White House, May 2011).

Office of General Counsel, *An Assessment of International Legal Issues in Information Operations* (U.S. Department of Defense, May 1999).

Orji, Uchenna J., "An Analysis of China's Regulatory Response to Cybersecurity", *Computer and Telecommunications Law Review* 7 (2012).

Orji, Uchenna J., *Cybersecurity Law and Regulation* (Wolf Legal Publishers, 2012).

Rauscher, Karl Frederick and Yaschenko, Valery, *Russia-U.S. Bilateral on Cybersecurity- Critical Terminology Foundations* (EastWest Institute and the Information Security Institute of Moscow State University, 2011).

Rauscher, Karl Frederick and Yonglin, Zhou, *China-U.S. Bilateral on Cybersecurity: Fighting Spam to Build Trust* (EastWest Institute, 2011).

Reich Pauline C., et al, "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity", *European Journal of Law and Technology*, 1(2)(2010).

Rollins, John and Wilson, Clay "Terrorist Capabilities for Cyber attack: Overview and Policy Issues" (RL 33123, CRS Report for Congress, January 22, 2007).

Romano, Cesare P.R., *The Peaceful Settlement of International Environmental Disputes: A Pragmatic Approach* (Kluwer Law International, 2000).

Schjølberg Stein, "The History of Global Harmonization on Cybercrime Legislation - the Road to Geneva" (unpublished, December 2008).

Schjølberg, Stein, "Terrorism in Cyberspace – Myth or reality?" (NATO Advanced Research Workshop on Cyberterrorism, Sofia, Bulgaria (October 2007).

Schjølberg, Stein, "Wanted: A United Nations Cyberspace Treaty" in *Global Cyber Deterrence: Views from China, U.S., Russia, India, and Norway* (Andrew Nagorski, ed., East West Institute, 2010).

Schwalb, Micah, "Exploit Derivatives and National Security", *Yale Journal of Law and Technology* 9 (2007).

Sofaer, Abraham D., et al**,** "A Proposal for an International Convention on Cyber Crime and Terrorism" (unpublished, August 2000).

Sofaer, Abraham D. "Towards an International Convention on Cyber Crime" in *The Transnational Dimension of Cyber Crime and Terrorism* (Goodman, Seymour E. and Sofaer, Abraham D., eds., Hoover Institution Press, 2001).

Sosa, Gilbert C., "Country Report on Cybercrime: The Philippines" (UNAFEI, 140th International Training Course Participants' Papers, undated).

Sprinkel, Shannon C., "Global Internet Regulation: The Residual Effects of the 'I LOVEYOU' Computer Virus and the Draft Convention on Cyber-Crime", *Suffolk Transnational Law Review* 25 (2002).

The Blacks Law Dictionary (8th Edition: West Group, 2004).

"The Trail Smelter Arbitral Decision", *American Journal of International Law* 35 (1941).

The Council of Europe, "Convention on Cybercrime" 41 I.L.M. 282 (Budapest, 23.XI, 2001).