JOURNAL OF ANTI-CORRUPTION LAW
2019 Volume 3 Pages 99 - 116

CYBERCRIME PROLIFERATION, INSTITUTIONS AND POLICIES: HANDWRINGING FOR CYBERCITIZENS

Felix E Eboibi*

ABSTRACT

Legal frameworks and policies on cybercrime operate at different levels and involve several institutions. These include constitutional and regulatory provisions, as well as statutory schemes that can affect cybercrime from global, multilateral, bilateral, national, regional and local perspectives. The current spate of cyber attacks and cyber criminality is alarming and is of great concern for cybercitizens globally. Unfortunately, the extant legal frameworks for cybercrime are not able to deal with the sophistication and techniques of cybercrime perpetrators. This paper examines the cybercrime conspiracy regime of certain governments as the basis of recent cybercrime proliferation globally and decries the unpreparedness and inability of the existing national and international legal cybercrime frameworks to rise to the challenge. It therefore proposes an international criminal law approach for curtailing the ever-increasing menace of cybercrime.

1 INTRODUCTION

The global development of information and communication technology (ICT) has paved the way for cybercriminals to engage in nefarious activities against innocent citizens who carry out legitimate business in cyberspace (cybercitizens).[1] A cybercrime is a crime perpetrated with the use of a computer either as a tool or target or against technology infrastructure. Connectivity to cyberspace readily

* PhD (Law), LLM (Nig.), LLB(Cal), BL(Nigerian Law School); Cybercrime Law Expert, Certified Digital Forensics Examiner; Senior Lecturer, Faculty of Law, Niger Delta University, Wilberforce Island, Nigeria. E-mails: *felixeboibi@mail.ndu.edu.ng or lixboibi@yahoo.com*.

1 See Brenner SW (2007) "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare" 97 *Journal of Criminal Law & Criminology* 379-476 at 381.

facilitates the ability of cybercriminals to commit offences which extend beyond national boundaries.[2]

The global digital population comprises in excess of 4.2 billion active internet users and 3.4 billion social media users. China, India and the United States of America (US) have the highest number of internet users.[3] From a regional perspective, East Asia accounts for 947 million internet users, followed by Southern Asia with 673 million internet users.[4] In Nigeria, internet users have increased rapidly, from 51.8 million in 2013 to 84.3 million in 2018. This figure is projected to grow to 93 million in 2019.[5] The total number of global mobile connections in 2018 was 8.5 billion,[6] with predictions that they would reach about 9.02 billion by 2020.[7] According to Nielson, the data service that is most used in the world today is the short message service (SMS).[8] Portio Research notes that about 8.3 trillion SMS messages would have been sent globally in 2018, with a total of 23 billion per day or about 16 million per minute.[9] Radicati broke down in detail the daily email traffic, reporting that about 124.5 billion business emails are sent and received per day, while consumer emails sent and received per day reach about 111.1 billion.[10]

What the above statistics portend is the potential increased use of ICTs in the facilitation of cybercriminality against cybercitizens. The perpetration of cybercrimes has been attributed to the ease of access to the internet, the

---

2 See Boateng R (2011) "Sakawa — Cybercrime and Criminality in Ghana" 11(2) *Journal of Information Technology Impact* 85-100 at 86; Shiryaev Y (2012) "Cyber Terrorism in the Context of Contemporary International Law" 14 *San Diego International Law Journal* 139-192 at 170.

3 Statista "Worldwide Digital Population as of July 2018", available at *https://www.statista.com/statistics/617136/digital-population-worldwide/* (visited 17 January 2019).

4 Statista "Number of Internet Users Worldwide 2018, by Region", available at *https://www.statista.com/statistics/249562/number-of-worldwide-internet-users-by-region/* (visited 14 August 2018).

5 Statista "Nigeria: Number of Internet Users 2013-2019", available at *https://www.statista.com/statistics/183849/internet-users-nigeria/* (visited 14 August 2018).

6 Statista "Global Mobile Connections from 2008 to 2020", available at *https://www.statista.com/statistics/371828/worldwide-mobile-connections/* (visited 14 August 2018).

7 Statista "Global Mobile Connections from 2008 to 2020".

8 Cited in SMSEagle (6 March 2017) "Daily SMS Mobile Usage Statistics", available at *https://www.smseagle.eu/2017/03/06/daily-sms-mobile-statistics/* (visited 14 August 2018).

9 Cited in SMSEagle (6 March 2017).

10 Cited in Campaign Monitor (March & May 2019) "Shocking Truth about How Many Emails are Sent", available at *https://www.campaignmonitor.com/blog/email-marketing/2018/03/shocking-truth-about-how-many-emails-sent* (visited 14 August 2018).

anonymity offered by the internet, the availability of e-mail extractor software/sites on the internet, ignorance of the gravity of breaking the law online, the precarious economic conditions of the people, and inadequate law enforcement.[11]

Despite their obvious impact on cybercitizens, it is mistakenly assumed sometimes that cybercrimes are victimless. Cybercrime inflicts physical, emotional and financial trauma on cybercitizens as victims.[12] Government institutions, businesses, schools, and the like are susceptible to global financial losses due to computer breaches. Cybercrime harms cybercitizens as it causes loss of value in safety, peace, money and property. Cybercitizens who engage in online shopping, electronic commerce and internet business activities have safety concerns about breaches of consumer privacy and information, resulting in their losing confidence in the internet. Cybercrime victims suffer emotional impact; they feel angry, cheated and blame themselves, especially when they realise that cybercrime perpetrators likely will go scot free, thereby denying them justice. Moreover, the proliferation of cybercrime has prompted corporations to incur costs to protect themselves from cybercriminals through the identification of risks, the assemblage of new and safer operating systems, and the purchase of riskless hardware and software.[13] The irony is that the costs expended by these corporations are passed on to consumers in the form of price increases for goods and services.[14]

---

11 See generally Eboibi FE (2018) "Introduction to Law & Cybercrime" in Eboibi FE (ed) *Handbook on Nigerian Cybercrime Law* Benin: Justice Jeco Printing and Publishing Global at 212-213; Crilley K (2001) "Information Warfare: New Battlefields — Terrorists, Propaganda and the Internet" 53(7) *Aslib Proceedings* 250-264; Ayantokun O (2006)"Fighting Cybercrime in Nigeria", available at *https://seclists.org/isn/2006/Jun/29* (visited 18 June 2020); Adomi EE (2005) "Internet Development and Connectivity in Nigeria" 39(3) *Program* 259-268; Nijboer J (2004) "Big Brother versus Anonymity on the Internet: Implications for Internet Service Providers, Libraries and Individuals since 9/11" 105 (1202/1203) *New Library World* 256-261; Weimann GO (2004) "How Modern Terrorism uses the Internet", available at *https://www.usip.org/sites/default/files/sr116.pdf* (visited 18 June 2020).

12 See Dallaway E (12 September 2016) "ISC2 Congress: Cybercrime Victims Left Depressed and Traumatized" Orlando, Florida, (Info Security), available at *https://www.infosecurity-magazine.com/news/isc2congress-cybercrime-victims/* (visited 14 May 2018); Urbelis A (2005) "Toward a More Equitable Prosecution of Cybercrime: Concerning Hackers, Criminals, and the National Security" 29 *Vermont Law Review* 975-1008 at 988; Hatfield M (2018) "Cybersecurity and Tax Reform" 93 *Indiana Law .Journal* 1161-1209 at 1162–1163 & 1168-1178; Payne BK (2018) "White-Collar Cybercrime: White-Collar Crime, Cybercrime, or Both?" 19 *Criminology, Criminal Justice, Law & Society* 16-32 at 20.

13 See Shiryaev, (2012) at 154.

14 Das S & Nayak T (October 2013) "Impact of Cyber Crime: Issues and Challenges" 6(2) *International Journal of Engineering Sciences & Emerging Technologies* 142-153 at 150.

According to Norton, around 65% of adults globally have been victims of cybercrime.[15] This figure underscores the enormity of this universal digital scourge. Cybercitizens largely are helpless and most perpetrators escape justice despite their criminal acts.[16] The proliferation of cybercrime and its impact is likely to continue until a lasting solution is found at both domestic and international levels. The 2017 Internet Crime Report shows the drastic level of global proliferation of cybercrimes from 2013 to 2017, as is evident from the table below.[17] Both the number of cybercrime complaints and the volume of losses grew steadily from one calendar year to the next.[18]

Global Proliferation of Cybercrimes: 2013-2017

Year	Number of Complaints	Volume of Losses Recorded
2013	262 813	$781.8 million
2014	269 422	$800.5 million
2015	288 012	$1 070.7 million
2016	298 728	$1 450.7 million
2017	301 580	$1 418.7 million
Total	1 420 555	$5.52 billion

Source*:* 2017 Internet Crime Report

The basic requirement for a globally effective and efficient curtailment of cybercrime is a legal framework that establishes specialised cybercrime regulatory institutions which can guide policy-making, ensure adequate legislation and promote law enforcement. In turn, the essence of a cybercrime legal framework is the creation of government agencies, institutions and bodies to regulate and

15 Symantec Corporation (US) "Norton Cybercrime Report: The Human Impact", available at *https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf* (visited 15 May 2018).

16 See Wolf JB (2000) "War Games Meets the Internet: Chasing 21st Century Cybercriminals with Old Laws and Little Money" 28 *American Journal of Criminal Law* 99-100; Symantec Corporation (US) "Norton Cybercrime Report: The Human Impact"; Shackelford SJ & Andres RB (2011) "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem" 42 *Georgetown Journal of International Law* 971-1016 at 979.

17 FBI internet Crime Complaint Center (2017) "Internet Crime Report" at 4, available at *https://pdf.ic3.gov/2017_IC3Report.pdf* (visited 24 October 2018).

18 FBI internet Crime Complaint Center (2017) at 4.

monitor what happens in cyberspace.[19] A regulatory framework should provide also for research, education and capacity building on cybercrime and its impact. In addition, such a framework should provide guidance on proper and appropriate behaviour in cyberspace for cybercitizens.[20]

The global rise of cybercrime has put regulatory frameworks under severe pressure. In 2018, the World Economic Forum ranked cybercrime amongst the top three global risks linked to the proliferation of the advanced technology.[21] Information on national regulatory frameworks for cyberspace is either sparse or difficult to obtain. And yet, analysing the existing regulatory frameworks is critical to understanding their efficacy.[22] In this regard, identifying a nation's cybercrime legal framework, policy and institutions and retrieving necessary facts could be of immense assistance in understanding cybercrime trends, confronting current loopholes and challenges, and crafting solutions.[23]

Many nations have developed legal frameworks to curtail the menace of cybercrime through the provision of cybercrime institutions and policies. One hundred and thirty eight countries (95 of them are developing and transition economies) have enacted cybercrime legislation, but more than 30 countries are yet to enact such legislation.[24] Overall, 72% of countries across the world have cybercrime legislation, 9% have draft cybercrime legislation and 18% have no cybercrime legislation.[25]

This paper argues that the recent proliferation of cyber criminality globally is not due necessarily to the absence of a cybercrime legal framework; nor to the ease of access to the internet, the anonymity offered by the internet, the availability of e-mail extractor software/sites, ignorance of the gravity of breaking the law online, the economic hardships of the people, or inadequate law enforcement. Rather, it is due to the adoption by nations of cybercrime conspiracy regimes. This refers to certain nations and governments sponsoring cybercrimes

---

19 FAO (2006) "Legal, Policy and Institutional Framework: Background Paper to the Kotka V Expert Consultation", available at *http://www.fao.org/forestry/10779-077da3d388bb2e60a5d98126bf5eee182.pdf* (visited 16 May 2018).

20 FAO (2006).

21 Jay J (17 January 2018) "Cybercrime Ranks among Top Three Global Risks in 2018, Says WEF Report", available at *https://www.teiss.co.uk/news/cyber-crime-top-global-risk-wef/* (visited 17 May 2018).

22 Jay (17 January 2018).

23 Jay (17 January 2018).

24 UNCTAD "Cybercrime Legislation Worldwide", available at *https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx* (visited 12 October 2018).

25 UNCTAD "Cybercrime Legislation Worldwide".

against fellow nations, governments and cybercitizens and, subsequently, shielding the perpetrators of cybercrimes from investigation and prosecution.[26] The paper recognises the inability of the existing cybercrime legal frameworks (domestically and internationally) to deal with this situation and advocates an international criminal law approach to hold individuals, nations and governments criminally responsible.

2 NATIONS AND THE CYBERCRIME CONSPIRACY REGIME

With the incessant growth of cyber criminality globally, cyber-attacks have metamorphosed into the gravest threat to humankind since nuclear weapons.[27] Money allocated to cybersecurity has tripled as nations seek to protect cybercitizens. The US Government spent $66 billion on cybersecurity in 2018, which is a substantial increase from the $27.4 billion it expended in 2010.[28] In 2017, about 700 million cybercitizens were victims of cybercrime in 21 countries. Globally, the estimated cost of cybercrime is $500 billion, while the cost of data intrusions against average corporations is estimated at $3.8 billion.[29]

Recent global trends have shown that cybercriminals are not acting on their own but enjoy the sponsorship of several nations or states.[30] When nations or states sponsor cybercriminals, the latter automatically are shielded from investigation and punishment.[31] Moreover, the immense assistance, resources and support which cybercriminals receive from governments afford them unprecedented access, expertise and talent.[32]

---

26 Brenner (2007) at 423.

27 Mason J "Cyber Security Statistics", available at *file:///E:/Cybercrime%20Institutions%20&%20Impact%20on%20cybercitizens/21%20Interesting%20Cyber%20Security%20Statistics%20(2017-2018)%20-%20TheBestVPN.com.htm* (visited 2 October 2018).

28 Statistica "Spending on Cybersecurity in the United States from 2010 to 2018", available at *https://www.statista.com/statistics/615450/cybersecurity-spending-in-the-us/* (visited 2 October 2018).

29 Comparitech (2018) "100+ Terrifying Cybercrime and Cybersecurity Statistics & Trends", available at *https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/* (visited 2 October 2018).

30 Shackelford & Andres (2011) at 973.

31 See Brenner, (2007) at 422; Shackelford & Andres (2011) at 974 & 975.

32 See Beard JM (2014) "Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target under International Humanitarian Law" 47 *Vanderbilt Journal of Transnational Law* 67-144 at 90; Van Hooijdonk R, "Cybercrime may be the Biggest Global Threat of 2018", available at *https://www.richardvanhooijdonk.com/en/blog/cybercrime-may-be-the-biggest-global-threat-of-2018/* (visited 16 May 2018).

North Korea is seen as one of the major sponsors of global cybercrime, apparently motivated by the impact of economic sanctions imposed by the UN Security Council, the European Union, the US, South Korea, Japan, Australia and others for its persistent involvement in the development of nuclear weapons and a ballistic missile technology programme.[33] In response, the North Korean government has resorted to backing professional cyber attackers and hackers to generate the funds needed to pilot its affairs.[34] Denning notes that since North Korea restricts access to the internet for the advantage of the elite, "it seems unlikely the country has hackers who operate independent of the government" and that the hackers "work primarily for the General Bureau of Reconnaissance or the General Staff Department of the Korean People's Army".[35] The February 2016 cyber attack on the Bangladesh Central Bank, alleged to have been masterminded by the North Korean regime, exemplifies nations conspiring with cybercriminals to offend freely in cyberspace, without fear of any punishment whatsoever.[36] This criminal collaboration might serve as an encouragement to perpetrators globally to continue to attack cybercitizens, which remains a major concern for the international community.

The Bangladesh attack involved the successful digital breach of the global SWIFT financial network. The attackers attempted to spirit away $951 million, but succeeded in transferring only $81 million.[37] Soon after this attack, there were

---

33 See Meginley CJ (2018). "The North Korean Crimes against Humanity: Establishing Legal Justification for International Military Action" 4(1) *Journal of Global Justice and Public Policy* 1-51 at 21-22; Albert E "What to Know About the Sanctions on North Korea", available at *https://www.cfr.org/backgrounder/what-know-about-sanctions-north-korea* (visited 8 October 2018).

34 See Siers R (2017) "North Korea: The Cyber Wild Card 2.0" 6(1) *Journal of Law & Cyber Warfare* 155-165 at 156, 157 & 160; Siers R (2014) "North Korea: The Cyber Wild Card" 4(1) *Journal of Law & Cyber Warfare* 1-12 at 4, 6 & 7; Denning D (20 February 2018) "North Korea's Growing Criminal Cyberthreat" *The Conversation,* available at *https://theconversation.com/north-koreas-growing-criminal-cyberthreat-89423* (visited 10 October 2018); Perlroth N & Corkery M "North Korea Linked to Digital Attacks on Global Banks" *The New York Times*, available at *https://www.nytimes.com/2016/05/27/business/dealbook/north-korea-linked-to-digital-thefts-from-global-banks.html* (visited 10 October 2018); Newsweek.com "North Korean Hackers Stole Over $1 Billion and Destroyed Computers around the World, Reports Reveal", available at *http://news-af.op mobile.opera.com/news/detail/3c1ddabd91449af7defaa7554062497e_ng?share=1&country=ng&language=en* (visited 4 October 2018).

35 Denning D (20 February 2018).

36 Denning D (20 February 2018).

37 Denning D (20 February 2018); Vaas L (14 March 2016) "Hacker's Typo Trips the Alarm on Billion-Dollar Cyber Bank Heist" *Naked Security,* available at *https://nakedsecurity.sophos.com/2016/03/14/hackers-typo-trips-the-alarm-on-billion-dollar-cyber-bank-heist/* (visited 27 September 2018).

similar attacks upon other banks. For instance, sometime in January 2015 the Ecuadorean *Banco del Austro* was attacked by hackers sneaking into the SWIFT network, which resulted in the transfer of several millions of dollars from the bank to other accounts globally.[38]

Researchers have confirmed that the two previous attacks on Sony in 2014[39] and South Korea in 2013 were similar in execution to the Bangladesh attack, thereby buttressing the suspicion that North Korea's "Lazarus Group" was the architect of all three attacks.[40] These kinds of attacks are capable of causing a global financial downturn if cybercriminals target financial institutions and their customers.[41]

United States v Park Jin Hyok is a recent criminal complaint filed by the US Department of Justice in the Los Angeles Federal Court against Park Jin Hyok, alleged to be a North Korean regime-backed programmer, for being involved in a series of cyber attacks.[42] The case testifies to the rise of state-sponsored cyber criminality globally.[43] It is alleged that Park was part of the "Lazarus Group"(also known as Guardians of Peace or Hidden Cobra), a hacking team whose aim was to execute cyber activities for and on behalf of the Democratic People's Republic of Korea (DPRK). The complaint decried the involvement of Park and the Lazarus Group in the Sony Pictures Entertainment cyber-attack in November 2014 — a reprisal for the movie *The Interview* — as well as the heist at the Bangladesh Bank. The complaint also revealed the Group's involvement in other bank heists in other countries between 2015 and 2018, using similar methods. It was alleged also that in 2016 and 2017, the cyber hackers trailed US defence contractors. In relation to the WannaCry 2.0 incident of May 2017, it was alleged that Park and his team developed a malware, in addition to two previous categories of ransomware, that

38 Perlroth & Corkery "North Korea Linked to Digital Attacks on Global Banks".

39 Henriksen A (2015) "Lawful State Responses to Low-Level Cyber-Attacks" 84(2) *Nordic Journal of International Law* 323-351 at 324-325, 340 & 342.

40 Siers (2017) at 161; Perlroth & Corkery "North Korea Linked to Digital Attacks on Global Banks".

41 Siers, (2014) at 3; Mee P & Schuermann T (2018) "How a Cyber Attack Could Cause the Next Financial Crisis", available at *https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis* (visited 3 June 2019); Wyman O (March 2018) "Large-Scale Cyber-Attacks on the Financial System: A Case for Better Coordinated Response and Recovery Strategies", available at *https://www.oliverwyman.com/.../oliver-wyman/.../2018/march/Large-Scale-Cyber-At.*. (visited 3 June 2019).

42 US District Court Central District of California, MJ 18-1479, Criminal Complaint, 8 June 2018, available at *https://www.justice.gov/opa/press-release/file/1092091/download* (visited 23 July 2019).

43 See generally Zagaris B (2018) "Cybercrime: US Unseals Criminal Complaint against N. Korean Programmer for Cyber Attacks and Intrusions" 34(9) *International Enforcement Law Reporter* 510-512; Vaas (14 March 2016).

contaminated and resulted in grave damage to several computers globally, including the incapacitation of computers at the UK's National Health Service. The complaint detailed how Park and his group were linked to the cybercrimes through emails and interconnected social media accounts that were used in sending spear-phishing messages. It also pointed out the use of common North Korea, Chinese and other IP addresses.[44] The US Assistant Attorney General stated thus:

> The complaint alleges that the North Korean government, through a state-sponsored group, robbed a central bank and citizens of other nations, retaliated against free speech in order to chill it half a world away, and created disruptive malware that indiscriminately affected victims in more than 150 countries, causing hundreds of millions, if not billions, of dollars' worth of damage. The investigation, prosecution, and other disruption of malicious state-sponsored cyber activity remains among the highest priorities of the National Security Division and I thank the FBI agents, DOJ prosecutors, and international partners who have put years of effort into this investigation.[45]

The investigation of Park's cyber atrocities was made possible only after he decided to part ways with the "Lazarus Group" where the North Korean government had afforded him maximum protection. The fact that no other members of the "Lazarus Group" are named in the criminal complaint lends credence to the idea that Park previously was protected.

Whereas North Korea's involvement in cybercrime supposedly is due to its very poor economic situation,[46] cybercrime has been devised as a deadly digital weapon by other nations to execute geopolitical claims and conflicts.[47] Reports have raised suspicions about Russian support for a number of attacks in Ukraine,[48] geared towards dampening political support for Ukraine's leaders and undermining public services.[49] Recently, it was alleged that Ukraine's National Postal Service, *Ukroposhta*, was subjected to ransomware and distributed denial of service (DDOS) attacks. This was similar to the 2015 Kiev power grid hacking, which reportedly was

---

44 US District Court Central District of California, MJ 18-1479, Criminal Complaint, 8 June 2018.

45 Cited in Vaas (14 March 2016).

46 Zagaris (2018) at 512.

47 Van Hooijdonk "Cybercrime may be the Biggest Global Threat of 2018".

48 Van Hooijdonk "Cybercrime may be the Biggest Global Threat of 2018"; Matwyshyn AM (2017) "Cyber" 5 *Brigham Young University Law Review* 1109-1196 at 1132; Shackelford SJ *et al* (2017) "From Russia with Love: Understanding the Russian Cyber Threat to US Critical Infrastructure and What to Do about It" 96(2) *Nebraska Law Review* 320-338 at 324-325 & 327.

49 Van Hooijdonk "Cybercrime may be the Biggest Global Threat of 2018"; Matwyshyn (2017) at 1132; Shackelford *et al* 324-325 & 327.

traced to computers with Russian IP addresses, implying that the attack was executed under the auspices of the Russian government.[50]

Another example of the rise of nations sponsoring cybercriminality from the perspective of geopolitical contestation is the alleged Russian involvement in the build-up to and aftermath of the 2016 US presidential elections. Research has shown that the US intelligence community investigated and discovered that cybercriminals, operating under the auspices of the Russian government, procured and sustained entry into the US state or local infrastructural electoral systems and consequently stole information or data pertaining to some 500 000 voters.[51]

The international community must not lose sight of the debilitating impact of these rising cybercrimes on cybercitizens. Retaliation by victimised states and their allies can spark off uncontrolled cyber-attacks which may culminate in cyber-warfare amongst states.[52] This becomes even more worrisome with the recent US announcement of a new cyber strategy mandating the Department of Defense to "defend forward" or "hack back" any prior or premeditated cyber-attack perpetrated against US critical infrastructures or networks. without the approval of the President's National Security Council.[53] By implication, the US military is

50 BBC News (10 August 2017) "Ukrainian Postal Service Hit by 48-hour Cyber-Attack", available at *https://www.bbc.com/news/technology-40886418* (visited 9 October 2018); Greenberg A (6 December 2017) "Crash Override: The Malware that Took Down a Power Grid" *Wired*, available at *https://www.wired.com/story/crash-override-malware/* (visited 9 October 2018).

51 Matwyshyn (2017) at 1116; Shackelford *et al* (2017) at 323-324; Norden L (16 July 2018) "Mueller's Latest Indictment Suggests Russia's Infiltration of US Election Systems Could Get Worse" *Brennan Center for Justice,* available at *https://www.brennancenter.org/mueller-latest-indictment-suggests-russia-infiltration-us-election-systemsworse?utm_source=twitter&utm_medium=socialmedia* (visited 11 October 2018); Vaas L (17 July 2018) "Twitter Shutters Accounts Linked to US Election Hacking" *Naked Security*, available at https://nakedsecurity.sophos.com/2018/07/17/twitter-shutters-accounts-linked-to-us-election-hacking/ (visited 11 October 2018); Vaas L (10 September 2018) "'Only Paper Ballots by 2020!' Call Experts after Election Tampering" *Naked Security*, available at *https://nakedsecurity.sophos.com/2018/09/10/only-paper-ballots-by-2020-call-experts-after-election-tampering/* (visited 10 October 2018); Naylor B (23 March 2018) "Russia Hacked US Power Grid — So What Will The Trump Administration Do About It?" *National Public Radio*, available at *https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the-trump-administration-do-about-it* (visited 11 October 2018).

52 Shackelford & Andres (2011) at 978.

53 Thomsen J (19 September 2018) "New Defense Cyber Strategy Gives Military Power on Preventative Cyberattacks" *The Hill*, available at *https://thehill.com/policy/cybersecurity/407389-new-defense-cyber-strategy-gives-military-power-on-preventative* (visited 11 October 2018); Vaas L (20 September 2018) "US Military Given the Power to Hack Back/Defend Forward" *Naked Security*, available at *https://nakedsecurity.sophos.com/2018/09/20/us-military-given-the-power-to-hack-back-defend-forward/* (visited 11 October 2018).

empowered to launch preventive cyber-attacks to thwart cyber-attacks against the US, her allies and partners in defence of critical infrastructures and networks.

Offensive cyber-attacks against another country's critical infrastructure would cause severe injury to that country's cybercitizens and civilian critical infrastructures, in flagrant breach of the United Nation's consensus against harming civilian critical infrastructure during peacetime.[54] For instance, where a cyber-attack is made against a country's critical infrastructure with the use of weapons and devices which cause death, serious bodily injury or substantial damage to property, the United Nations International Convention for the Suppression of Terrorists Bombings would apply.[55] Such an attack is also a violation of the principle of prohibition on the use of force and non-intervention enshrined in international law by virtue of the United Nations Charter.[56] The UN Charter restrains a state from using force against the territorial integrity or political independence of another state. Article 2(4) states that:

> All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations.

Moreover, the debilitating nature of cybercrimes or cyber-attacks prompted the UN General Assembly to pass resolutions to maintain cybersecurity and to enjoin member states[57] from carrying out cyber activities in such a way that the rights of other states are jeopardised or affected adversely.[58]

---

54 Beard JM (2014) "Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law" 47 *Vanderbilt Journal of Transnational Law* 67-144 at 78; Council on Foreign Relations (23 July 2015) "Cyber Norm Development and the Protection of Critical Infrastructure", available at *https://www.cfr.org/blog/cyber-norm-development-and-protection-critical-infrastructure* (visited 11 October 2018).

55 See Council on Foreign Relations (23 July 2015).

56 See Council on Foreign Relations (23 July 2015); Kinacioglu M (2005) "The Principle of Non-Intervention at the United Nations: The Charter Framework and the Legal Debate" *Perceptions* 15-39.

57 Russia, China, Korea and the US are all member states of the UN. These countries are or have been accused previously of being involved state-sponsored cyber-attacks.

58 See Preambles to Resolutions A/RES/55/28 of 20 November2000; A/RES/56/19 of 29 November 2001; A/RES/59/61 of 3 December 2004; A/RES/60/45 of 8 December 2007; A/RES/61/54 of 6 December 2004; A/RES/62/17 of 5 December 2005; A/RES/61/54 of 6 December 2006; General Assembly Resolution A/RES/64/25 of 2 December 2009. See also Beard (2014) at 89.

3 USING INTERNATIONAL CRIMINAL LAW TO ADDRESS CYBER CRIMINALITY

To put an end to the proliferation of state-sponsored cybercrimes, the honest co-operation of the international community cannot be over-emphasised. Urgent international criminal law steps[59] must be taken to punish nations perpetrating and backing professional cybercriminals, for whatever reason, and to ensure that states do not become safe havens for cybercrime perpetrators.[60]

Unfortunately, the present global cybercrime policies are not helpful in the investigation and prosecution of heads of state who are involved directly in sponsoring and shielding cybercriminals.[61] Existing laws, such as the US Computer Fraud and Abuse Act of 1986 (CFAA), the UK Computer Misuse Act of 1990, the UK Police and Justice Act of 2006, the UK Serious Crime Act of 2007, the Nigerian Cybercrimes (Prohibition, Prevention, Etc) Act of 2015, the AU Convention on Cyber Security and Personal Data Protection, and the Council of Europe Convention on Cybercrime, do not envisage holding sitting heads of state and governments accountable for their role in cybercrime proliferation.[62] This is evident from the US indictment of Park Jin Hyok, which did not extend to the head of the North Korean government. However, such an extension would be a breach of the general criminal law principle of *nullum crimen sine lege* or the principle of legality. Acquaviva notes that:

> the purpose of *nullum crimen* is nowadays better described, however, as that of safeguarding individuals against the arbitrary power of prosecuting authorities and undue judicial discretion (hence the corollary of banning convictions on the basis of analogy).[63]

59 See Henriksen (2015) at 328.
60 See Beard (2014) at 77.
61 See Shiryaev (2012) at 156.
62 See Beard (2014) at 75; Shiryaev (2012) at 165.
63 Acquaviva G (2011) "At the Origins of Crimes against Humanity: Clues to Proper Understanding of the *Nullum Crimen* Principle in the Nuremberg Judgment," 9(4) *Journal of International Criminal Justice* 881-903 at 883-884. See also Ritter von Feuerbach PJA (2007) "Foundations of Criminal Law and the *Nullum Crimen* Principle" 5 *Journal of International Criminal Justice* 1005-1008 at 1008; Von Liszt F (2007) "The Rationale for the *Nullum Crimen* Principle" (2007) 5 *Journal of International Criminal Justice* 1009-1013 at 1009.

According to Canale & Tuzet:

> one argues analogically after having interpreted the relevant provisions and having established that the case is not regulated … by the law in the sense that no available interpretation of a valid legal provision has been able to set up a norm covering it.[64]

The extant global cybercrime legal frameworks do not make provision for holding heads of state and governments liable for their involvement in cybercrime or cyber-attacks. The omission can be cured only by prosecuting and judicial authorities resorting to analogical reasoning, which is forbidden by criminal law.[65]

However, the gap in national cybercrime legal frameworks does not exclude the applicability of international criminal law.

> A person may be held guilty of an act or an omission that was not punishable by the applicable national law at the time the offence was committed so long as this was punishable under international treaty law or customary law at the time the offence was committed.[66]

In the circumstances, this paper argues that resort should be had to the Rome Statute of the International Criminal Court. The aim of the Rome Statute is to ensure that all persons are equal before the law and should be punished for their crimes, regardless of their status. The involvement of heads of state and governments in the perpetration of cybercrime underscores the inability or unwillingness of national governments and courts to go against the perpetrators of this serious form of crime. The borderless nature of cybercrime and its global impact upon cybercitizens illustrate the international peculiarities of cybercrime, which deserves to be treated as an international crime by the international community. The preamble to the Rome Statute affirms:

---

64 Canale D & Tuzet G (2016) "Analogical Reasoning and Extensive Interpretation"at 4, available at *https://www.academia.edu/3623709/Analogical_Reasoning_and_Extensive_Interpretation* (visited 16 November 2019). See also Habibzadeh MJ (2006) "*Nullum Crimen, Nulla Poena Sine Lege*: With an Approach to the Iranian Legal System" 2 *International Journal of Punishment and Sentencing* 33-45 at 33.

65 Sieber U (2016) "The Paradigm Shift in the Global Risk Society: From Criminal Law to Global Security Law - An Analysis of the Changing Limits of Crime Control" 1 *Journal of Eastern-European Criminal Law* 14-17 at 17.

66 Nowak M (2005) *UN Covenant on Civil and Political Rights: CCPR Commentary* (2ed rev) Strasbourg: NP Engel at 281 cited in Acquaviva (2011) at 883-884. See also Chaumette AL (2018) "International Criminal Responsibility of Individuals in Case of Cyberattacks" 18 *International Criminal Law Review* 1-35 at 6; Pernice D (May 2015) "Critical Analysis of the Substance and Application of the Principle of Legality in International Criminal Law" at 4 & 12, available at *https://www.academia.edu/12427234/Critical_analysis_of_the_substance_and_application_of_the_principle_of_legality_in_international_criminal_law* (visited 14 November 2019).

> that the most serious crimes of concern to the international community as a whole must not go unpunished and that their effective prosecution must be ensured."

This ambition embodies the potential of the Rome Statute to put an end to the global cybercrime impunity by ensuring that its perpetrators are prosecuted.

The Rome Statute is the treaty that established the International criminal Court (ICC), the first treaty-based permanent international court that is capable of trying individuals accused of committing the most serious crimes, in violation of humanitarian and human rights law, namely, genocide, crimes against humanity and war crimes.[67] The perpetrators of these crimes may be heads of state, commanders of armed forces or members of parliament. Their official capacity does not exempt them from being criminally responsible under the Rome Statute.

Of course, cybercrime is not identified specifically as one of the crimes that may be prosecuted before the ICC. However, Article 7 of the Rome Statute provides for crimes against humanity and lists certain acts — in Article 7(1)(a)-(k) — which, "when committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack", amount to such crimes.[68] Although, cybercrime or cyber-attack is not listed, Article 7(1)(k) stipulates:

> other inhumane acts of similar character intentionally causing great suffering, or serious injury to body or to mental or physical health.

The expression "other inhumane acts" implies that the forms of conduct that may be regarded as inhumane are not exhaustive. Both the Rome Statute and the Elements of Crimes imply that the acts must take place as part of an attack.[69]

Cyber-attacks are hostile acts perpetrated through computer infrastructures with the aim of causing the destruction of the cyber systems of a country's computer infrastructure.[70] It is also an attack against a state's cyber network by or under the auspices of another state to cause damage to or disruption of the network.[71] Where the armed forces or any organ of a state carries out a cyber-attack or encourages another organisation to carry out the attack or the attack is carried out under the directives of the state or the state accepts an attack as its

---

67 See Articles 5-8 of the Rome Statute.

68 See Shiryaev (2012) at 173; Scharf MP & Newton MA (2011) "Terrorism and Crimes against Humanity" in Sadat LN (ed) *Forging a Convention for Crimes against Humanity* New York: Cambridge University Press at 267-269.

69 Article 7(1) of the Rome Statute; Elements of Crimes at 13.

70 Hathaway OA *et al* (2012) "The Law of Cyber-Attack" 100 *California Law Review* 817-885 at 817.

71 Hathaway *et al* (2012) at 817; Beard (2014) at 68-69.

own, such cyber-attack is attributed to such state.[72] A cyber-attack on computer infrastructures or systems impinges on the integrity, authenticity and availability of the computer infrastructure by altering the stored data in a computer system, manipulating the source of information and making a computer network inaccessible to the user.[73] It could also be an attack upon a computer system that affects the power grid or an attack upon the economic and political stability of a state.[74] Where cyber-attacks result in the death of persons and damage to property, they should be seen automatically as attacks in terms of international criminal law.

These attacks affect cybercitizens and the civilian population of a state, in terms of physical or mental integrity and health or human dignity and, consequently, qualify as attacks under Article 7 of the Rome Statute. Perpetrators of cyber-attacks are capable of inflicting great suffering or serious bodily or mental injury similar in gravity to the inhumane acts mentioned in paragraph 1 of Article 7.[75] Howard notes that, apart from financial loss, cybercrimes cause emotional and physical trauma:

> Victims often feel that there has been an invasion of privacy, people feel victimised, that they have suffered a traumatic experience; from behavioural standpoint of view, victims can suffer insomnia and eating disorders.[76]

Howard notes further that the threat to use data of cybercitizens stolen by perpetrators is even more traumatic than its happening in reality. She substantiates her position with reference to the Ashley Madison breach, where email threats were issued to expose a man who, in consequence, committed suicide:

> "His name was never actually leaked – this is an example of how the threat of a situation can be as distressful as the actual leaking of information."[77]

---

72 See Couzigou I (2018) "Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations" 32(2) *International Review of Law, Computers and Technology* 1-21 at 4; Article 4 of the Draft Articles on the Responsibility of States for Internationally Wrongful Acts; Tsagourias N (2012) "Cyber Attacks, Self-Defence and the Problem of Attribution" 17 *Journal of Conflict and Security Law* 229-244 at 237; Shackelford & Andres, (2011) at 975 & 989.

73 Solis GD (2014) "Cyber Warfare" 219 *Military Law Review* 1-52 at 6.

74 Lin HS (2010) "Offensive Cyber Operations and the Use of Force" 4 *Journal of National Security Law & Policy* 63-86 at 67.

75 Brenner (2007) at 391.

76 Cited in Dallaway (12 September 2016). See also Kobie N (4 December 2017) "The Emotional Burden of Being Hacked", available at *https://motherboard.vice.com/en_us/article/8xm4mv/the-emotional-burden-of-being-hacked-stressweek2017* (visited 17 October 2017).

77 Cited in Dallaway (12 September 2016). See also Beard, (2014) at 113.

The fact that a cyber-attack is perpetrated through the use of a computer does not prevent it from being a use of force or an armed attack.[78] Relying upon the judgment of the International Court of Justice in the Nicaragua case, the Tallinn Manual notes that a cyber-attack constitutes the use of armed force "when its scales and effects are comparable to non-cyber operations rising to the level of a use of force".[79] Based on the Elements of Crimes, reference to an "attack" does not automatically mean "military attack" under international humanitarian law.[80] It thus could include an operation against cybercitizens and a civilian population.[81] The participation of military forces or armed hostilities or any violent force at all is not necessary for such an operation to be equated to an attack for the purposes of international criminal law.[82] It could encompass any abuse or ill treatment of cybercitizens and civilians.[83] Moreover, the occurrence of the attack need not be related to armed hostilities or armed conflict.[84]

A vital issue embedded in Article 7 is the widespread and systematic nature of cybercrimes or cyber-attacks that are directed against a civilian population. A cyber-attack would be seen to be systematic where it shows a "non-accidental repetition of similar criminal conduct on a regular basis".[85] The alleged North Korean and other cyber-attacks mentioned earlier exemplify the intentional co-ordinated and organised nature of cyber-attacks, exhibiting common and similar modes of execution against their cybercitizen and civilian victims. Notable also is the widespread nature of the attacks on the civilian population across national borders. Knowledge of the large widespread or systematic character of the attack on cybercitizens and the civilian population by the perpetrator is a requirement under Article 7 of the Rome Statute. In this regard, the Elements of Crimes states:

78 Solis (2014) at 16.

79 Schmitt MN (ed) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2ed) New York: Cambridge University Press at 331.

80 Paragraph 3 of the Introduction to Article 7 of Elements of Crimes. See also Boot M *et al* (2008) "Article 7 – Crimes against Humanity" in Triffterer O (ed) *Commentary on the Rome Statute of the International Criminal Court: Observers Notes', Article by Article,* (2ed) Germany: Verlag CH Bech oHG) at 175.

81 Boot *et al* (2008) at 175.

82 Boot *et al* (2008) at 175.

83 Boot *et al* (2008) at 175.

84 Boot *et al* (2008) at 175.

85 ICTR *Prosecutor v Kordic,* Case No IT-95/14/2-A, Judgment, Appeals Chamber, 17 December 2004, paragraph 94; *Prosecutor v Blaskic,* Case No IT-95-14-A, Judgment, Appeals Chamber, 29 July 2004 paragraph 101.

> The perpetrator knew that the conduct was part of or intended the conduct to be part of a widespread or systematic attack against a civilian population.[86]

This requirement does not mean that the perpetrator must have knowledge of all details of the attack perpetrated[87] or that his or her actions were inhumane or rose to the level of a crime against humanity.[88] Actual or constructive knowledge is applicable here,[89] and in determining whether the perpetrator's act is a crime against humanity, his or her personal motives in taking part in the cyber-attack on a civilian population is irrelevant.[90]

Criminal investigation and prosecution may be pursued against individuals and heads of state and governments alleged to be perpetrators of cybercrimes or cyber-attacks under Article 7 of the Rome Statute via three routes: State Party referral; UN Security Council (UNSC) referral; and *proprio motu* referral by the ICC Prosecutor.[91] State Party referral involves a state party lodging a complaint with the ICC Prosecutor about an alleged cybercrime or cyber-attack as a crime against humanity, pursuant to Articles 13(a) and 14 of the Rome Statute. The UNSC is obligated to refer a situation to the ICC prosecutor where it observes that a cybercrime or cyber-attack relating to Article 7(k) has been committed. The UNSC would act in terms of Chapter VII of the Charter of the United Nations and pursuant to article 13(b) of the Rome Statute. Finally, where there is a cyber-attack, the ICC Prosecutor may act on his or her own initiative to launch an investigation and prosecution in accordance with Articles 13(c) and 15 of the Rome Statute.

4 CONCLUSION

The development of ICT globally has seen daily increases of cybercitizens who lack a universal pragmatic approach to curtail global cybercrime proliferation. To be sure, most nations and governments have developed cybercrime legal frameworks and policies to combat cybercrime proliferation. However, these global efforts have been negated recently by some nations and governments advancing the hand of fellowship to cybercriminals through sponsoring their cyber-related activities

---

86 Paragraph 4 of the Introduction to Article 7 of Elements of Crimes.

87 See Boot *et al* (2008) at 182 n 82.

88 See Boot *et al* (2008) at 182 n 82.

89 *Prosecutor v Tadic,* Case No IT-94-I-T, Opinion and Judgment, Trial Chamber, 7 May 1997, paragraph 657.

90 *Prosecutor v Tadic,* Case No IT-94-I-T, Opinion and Judgment, Trial Chamber, 7 May 1997, paragraph 657.

91 Article 13 of the Rome Statute. See also Eboibi FE (2017) "The Pre-trial Procedures and Principles of the International Criminal Court" 8(1) *Nnamdi Azikiwe University Journal of International Law and Jurisprudence* 74–82; Meginley (2018) at 24-25.

and shielding them from investigation and punishment. The corollary would be a continuous and consistent wave of cyber criminality and cyber-attacks against cybercitizens.

How long will the international community keep mute about this alleged state-sponsored cyber criminality and its proliferation globally? From a cybersecurity perspective, it is necessary for cybercitizens to avoid accessing files sent either as attachments or otherwise from untrusted sources, pending a global and definitive response to the incessant and co-ordinated waves of cyber-attacks.[92] Based on the foregoing, this paper suggests an international criminal law approach by deploying the resources of the Rome Statute of the International Criminal Court against cybercrime perpetrators, whether they be individuals or heads of state and governments. The realisation of this objective is possible only with the honest co-operation of the international community of states.

92 See Van Hooijdonk "Cybercrime may be the Biggest Global Threat of 2018".