Artha-Journal of Social Sciences
2020, Vol. 19, No. 4, 21-36
ISSN 0975-329X|https://doi: 10.12724/ajss.55.2

Digital World: Threats to Security and the Scope for South-South Cooperation

Cherian Samuel*

Abstract

Technological advances have had a tremendous impact on the development of economy and society in the twenty-first century albeit with several security threats as well which are yet to be regulated. Many factors contribute to digital threats, making countries vulnerable and insecure, ranging from a large number of users, the intrinsic lack of security architecture, and the global nature of cyberspace. Whilst much of the focus is on confidence-building to facilitate international co-operation to facilitate rules-of-the-road, capacity building is equally important, though not receiving adequate attention because of the focus on great power politics. For developing countries, there is a need to ramp up capacities to deal with cyber threats. There is much scope for South-South cooperation in this regard since many developing countries, including India, possess advanced digital capabilities.

Keywords: Digital threats, Co-operation, Digital divide, South-south co-operation, Capacity building, Cyberspace, Cyber threats, Vulnerabilities, Malware, Norms, Cybercrime, Cybersecurity, UNGGE, Paris Call

1. Introduction

For the developing countries, in particular, cyberspace has aided in development goals, increased connectivity, and has had a positive impact on various fields, from education, to financial inclusion and

* Research Fellow, Manohar Parikkar Institute for Defense Studies and Analyses, New Delhi, India; cherian.samuel@gmail.com

health. On the flip side, it has also led to destabilisation and increased vulnerabilities in many areas, resulting in threats to critical information infrastructure, an increase in cybercrime and cyber-enabled crime. Further, the dawn of global surveillance mechanisms, the militarization of cyberspace, and most recently, the absence of digital borders has created opportunities for various threat actors to create societal instability through fake news and so on.

The causes of the threats are the result of vulnerabilities in the software, hardware, networks and endpoints that make up the cyberspace. Whilst technical solutions have mitigated some of those threats, they can only go so far, given that there are millions of vulnerabilities and a strong criminal enterprise eco-system to monetise the sale and misuse of these vulnerabilities. The many users of this eco-system range from criminal enterprises to state and state-sponsored actors and even the gigantic transnational behemoths that make up the tech titans find themselves unable to match up to the collective might of the criminal enterprises ranged against them. Consequently, it falls on state institutions at a national and supra-national level to find ways and means of responding to digital threats. However, multi-lateral bodies that would traditionally be for a resolution of differences have been found wanting, partly because since cyber issues are not purely the concern of states but have multiple stake holders spread across a multitude of domain areas (Nye,2014).

2. The Digital Divide

However, what is often overlooked in the broader discussion of threats from the digital world is that developing countries are even more vulnerable to these threats than the developed countries. Many have lacked the resources and capabilities to ensure that their citizens can access these services safely. The digital divide manifests itself not just across countries and regions but even within countries with some states, even within India, having more capabilities and resources to deal with cyber threats more than others. These disparities have consequences not only for economic

growth but also provide opportunities for bad actors to take advantage of this borderless space.

Too often, the developing countries focus on subsets of cyberspace such as cybercrime and social media, rather than addressing the root cause of the vulnerabilities in cyberspace. The reasons for this are many. Cybercrime, as a case in point, fits within the existing responsibility of the law enforcement apparatus. Consequently, a lot of attention has gone into addressing the gaps, and there are many. Most cyber-crime is cross-border in nature, and there has been much discussion on the logistics of coordinating across borders to collect and retain digital evidence which is easily erased or can be subject to manipulation, as well as on more fundamental issues such as harmonisation of various laws in these countries to enable the law to take its course.

The global losses due to cybercrime have fluctuated widely since there is no verifiable method for measuring cybercrime. A 2018 report by McAfee in association with the Center for Strategic and International Studies gives a figure of $ 600 billion (Signé and signé, 2018). In addition to monetary loss, there are other losses including a reputational loss to businesses, loss due to theft of intellectual property, loss of productivity and legal costs.

Some aspects unique to developing countries are the low level of cyber literacy, especially at the level of individuals which makes them easy targets for all manner of social engineering-based crimes. Another aspect to be considered is the need to focus on mobile security as much as computer security given that most interactions and transactions in developing countries take place through mobile phones. Mobile vulnerabilities increased by 215% in 2015 over 2014 according to a report commissioned by the Global Forum on Cyber Expertise (Global Forum on Cyber Expertise, 2017). Low-income levels also are a cause of computer piracy, in turn leading to compromised systems which are then used for bot network activities. While botnet infections in India have come down after government-led initiatives such as the Cyber Swachhta project to clean computers, it is still ranked second in the list of botnet infected countries (The Spamhaus Project, n.d).

However, it is not just the vulnerabilities in the software but the use of those not just by cyber-criminals, but also state-sponsored actors for purposes ranging from espionage to attacks on critical information infrastructure. Attacks have ranged from ransomware attacks to Dedicated Denial of Service (DDOS) Attacks. Malicious ransomware attacks like Wannacry, Petya and Notpetya were rebuffed through a combination of luck and active response by governments and tech companies. Whilst Notpetya brought the operations of the shipping giant Maersk in India to a halt (Saul, 2017), several countries in Africa were impacted by the Wannacry ransomware (CIO East Africa, 2017). India was affected the most by NotPetya in the Asia-Pacific region and was the seventh most affected globally. Wannacry was formally attributed to North Korea by the US-supported by allies in December 2017 though North Korea rejected these allegations. While Petya's origins were murkier, like Wannacry, it was based on an exploit developed by the US National Security Agency (NSA) which was leaked in March 2017 by the Shadow Brokers, a hacking group believed to be affiliated to Russian intelligence. According to reports, North Korea is even using the proceeds of cyber-criminal activities carried out by its agents as a source of funding for its military and nuclear and missile programs. That much of this cannot be conclusively and independently verified speaks of the difficulties of applying traditional methods of security such as arms control and technology denial regimes since these rely on mechanisms centred around verifiability. Thus, cyber-attacks need not be targeted to be destructive, and more often than not, countries find themselves affected as collateral damage. For instance, although, Notpetya was targeted at Ukrainian infrastructure, the malware went viral and infected computers in more than 65 countries (Chappell, 2017). The absence of borders in cyberspace means that attackers can spoof their identities and even basic forensics to arrive at the source of the attacks is difficult. However, in the absence of viable alternatives, the technologically advanced powers, particularly the United States, are seen to be practising a modified form of "cyber" deterrence which focuses on imposing sanctions and punitive actions on individuals rather than countries (Braw, 2020). Whilst this approach has been criticised by some for placing too much

emphasis on the lower-level operational actors rather than the strategic masterminds behind these actions, others see this as the only way to go (Braw, 2020:49).

3. Defining Cybersecurity

Cybersecurity is much more than cybercrime, and discussion on the more fundamental issues is lacking as seen when examining even basic definitions which are largely borrowed from elsewhere. As far back as 2010, the United Nations Group of Governmental Experts (UNGGE) on Developments in the field of Information and Telecommunications in the context of International Security, had recommended "(v) Finding possibilities to elaborate common terms and definitions relevant to General Assembly resolution 64/25" in its report to the First Committee of the United Nations (United Nations, 2010a).

The term Cybersecurity is a dynamic concept that has evolved over the years from the techno-centric definition put out by the International Telecommunications Union to broader all-encompassing definitions such as the one put out by the US Department of Homeland Security. The ITU definition described Cybersecurity as follows:

> "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity, which may

include authenticity and non-repudiation, and Confidentiality." (ITU, n.d.)

The US Department of Homeland Security in its glossary of Cybersecurity Terminology defines cybersecurity as follows: "Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure" (Department of Homeland Security, n.d.). These differing, and sometimes conflicting definitions are present across the board with the basic conflict over what constitutes cyberspace, cybersecurity and other related terms yet to be resolved and the number of alternative definitions increasing by the year.

4. International Efforts

The establishment of the previously mentioned UNGGE on Developments in the field of Information and Telecommunications in the context of International Security was pursuant to a resolution moved by Russia in 1998 calling on the UN General Assembly to examine the issue of information security. The resolution invited member states to make known their views on information security, come up with basic definitions and ponder on the "advisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality" (United Nations, 1999).

The first group of governmental experts set up in 2004 by the First Committee, one of the UN General Assembly's six committees, on Disarmament and International Security, could not even arrive at a consensus on recommendations to be submitted to the 1st Committee, with vastly divergent positions taken by Russia and China on the one hand, and the US and its European allies on the other, on even the issues to be discussed by the GGE. The two-page

report to the Secretary-General simply noted that "given the complexity of the issues involved, no consensus was reached on the preparation of a final report" (United Nations, 2005).

In subsequent iterations, the basic pillars for securing cyberspace were conceptualised and sought to be fleshed out. The 2010 GGE Report recommended dialogue among States on the norms to address collective risks and for protecting the critical national and international infrastructure. It also called for measures to promote confidence, stability and risk reduction. The main achievement of the next GGE was to have an outcome document that recognised that existing international law applied to cyberspace. This, to an extent, settled the longstanding debate whether cyberspace required new laws taking cognisance of its unique attributes or whether existing laws were sufficient.

The subsequent GGE tried to push ahead on all these tracks; it examined how international law applies in cyberspace. It recommended voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful cyberspace. It further elaborated on confidence-building measures and capacity building in less developed countries. The GGE process seems to be on track with the recommendations of the 2015 GGE containing clauses that reflected concerns and priorities of various countries. Some clauses emphasised that state security must go hand-in-hand with respect for human rights and fundamental freedoms, others that States must not use proxies to mask their activities, and that they must ensure that their territories are not used by non-State actors for unlawful activities. It was agreed that state sovereignty in cyberspace applied to conduct of ICT-related activities, and states had jurisdiction over ICT infrastructure within their territory. However, despite the veneer of agreement, there were fault lines connected not just to cybersecurity but the changing geopolitical landscape and the 2016 GGE could not agree on a consensus report, dealing a body blow to the UNGGE process which had coalesced around rights and duties of states in cyberspace. While earlier GGEs had seen an agreement that both were to be derived from existing international law, the 2016 GGE had the crucial mandate of

taking the process forward and spelling out how the laws applied as well as fleshing out norms that would fill in the gaps. Further progress was stymied for several reasons including mutual suspicions on the parts of opposing blocs about the motivations and interests of the other. Even if there was no consensus agreement on the report, the report itself made some crucial recommendations structured around sharing information, state responsibility, Human rights, as well as protecting critical information infrastructure, supply chain integrity, CERT autonomy.

The eleven recommendations were:

a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;

b) In the case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

d) States should consider how best to cooperate to exchange information, assist each other, and prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;

e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age,

to guarantee full respect for human rights, including the right to freedom of expression;

f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

k) States should not conduct or knowingly support activity to harm the information systems of the authorised emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

However, even as it seemed that the GGE process had run its course, it was resurrected in 2018 when the UN First Committee of the General Assembly (GA) adopted two resolutions - one establishing the sixth UNGGE (to start in 2019 and report to the UNGA in 2021), the other establishing the new Open-Ended Working Group (OEWG) (to start in 2019, and report to the UNGA in 2020). Whilst the agenda of the former is to expand on the report and recommendations of previous GGEs, the OEWG is a different mechanism enough mechanism to be complementary and not an alternative to the UNGGE, even if their agendas were quite similar. The agenda of the UNGGE is as follows:

> to continue to study, to promote common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building, as well as how international law applies to the use of information and communications technologies by States, and to submit a report on the results of the study. (United Nations, 2018a)

The agenda of the OEWG is as follows:

> to further develop the rules, norms and principles of responsible behaviour of States, and the ways for their implementation; if necessary, to introduce changes to them or elaborate additional rules of behaviour; to continue to study, to promote common understandings, exist and potential threats in the sphere of information security and possible cooperative measures to address them and how international law applies to the use of information and communications technologies by States, as well as confidence-building measures and capacity-building and to submit a report on the results of the study to the General Assembly. (United Nations, 2018b)

The fundamental difference between the two is that the OEWG consists of all the member states of the United Nations while the UNGGE only has 25 members, selected in such a way as to give

equal representation to geographic regions. The OEWG is also a more open forum and has a mechanism for inputs by civil society organisations

5. Whither the voice of the emerging countries?

India has been a member of the UNGGE in the very first iteration that ran from 2004-05. It was also a member of the 2009-10, 2012-13, and 2016-17 Groups. That said, emerging country representation in this important apex body for cybersecurity and global internet governance has been quite limited. The 2004-05 grouping had Brazil, Belarus Jordan, Malaysia, Mexico, Mali and South Africa, 2009-10 had Belarus, Brazil, India, and South Africa, 2012-13 again had emerging country representation from Argentina, Belarus, Egypt, India, and Indonesia, while 2014-15 had Belarus, Brazil, Colombia, Egypt, Ghana, Kenya, Malaysia, Mexico, Pakistan, and the last iteration which had increased membership to 25 had 4 countries from Africa, Kenya, Egypt, Senegal and Botswana. Even if the representation has increased, the less affluent members have less capacity to address the multi-faceted and complex issues before the GGE and often defer to the arguments made by the big powers (Mueller, 2017).

Low representation by less developed countries is in contrast to many of the advanced middle powers like Australia, Netherlands, Germany and Switzerland who have astutely built-up capabilities and are projecting their positions to ensure a seat at the high table global cyber governance, if and when it fructifies. This extends from hosting global conferences on cyberspace to funding think-tank activities and building up offensive and defensive capabilities. This has already had results in the UN where these countries have invariably been part of successive GGEs over the years.

This asymmetric representation is not restricted to multi-lateral groupings but even in multi-stakeholder groupings such as the Internet Governance Forum in which according to a study in 2015 which looked at representation by geographies noted that representation from say, Africa stood at 14 % in the years 2010-15 at the annual meetings of the forum compared to 44% from Western

Europe. Even if cybersecurity issues have occasionally found their way into resolutions of developing country fora such as the G77, these have been episodic and unsustainable. Emerging countries have also tried to bring their priorities to the fore at ITU led fora such as the World Conference on International Telecommunications (WCIT) and the World Telecommunication Development Conference (WTDC), but these fora have inevitable been hijacked by the long-drawn out-conflicts between the authoritarian countries such as China and those countries opposed to them. The collapse of the World Conference on International Telecommunications (WCIT) held in December in 2012 is instructive in this regard. Russia and China were at the forefront of proposing various policy measures that ultimately serve to gain more control over their national cyberspace. Russia proposed under Article 8 that "Member States shall ensure unrestricted public access to international telecommunication services and the unrestricted use of international telecommunications, except in cases where international telecommunication services are used for the purpose of interfering in the internal affairs or undermining the sovereignty, national security, territorial integrity and public safety of other States, or to divulge information of a sensitive nature (Mueller, 2017)." Other countries pushed back, resulting in a stalemate with a significant number of countries refusing to ratify the resolutions to bring internet governance within the ambit of the International Tele-communications regulations. The same sequence of events again played out at the World Telecommunication Development Conference (WTDC) held in Buenos Aires in 2017 with the final consensus being to leave the 2014 resolution on cybersecurity unchanged. According to a report on the Conference, "WTDC's failure to reach agreement on cybersecurity—a topic that many other forums have also failed to reach consensus on—was framed, particularly by the African group, as an attack on the legitimate desire of developing countries to have the same level of development as developed countries (Mueller, 2017)."

5.1 Bridging the Digital Divide: India in Africa

India has been a strong votary of South-south co-operation which refers to technical cooperation among the developing countries in

the Global South. In a speech to the Ugandan Parliament in 2018, Prime Minister Narendra Modi had spelt out India's guiding principles for South-South co-operation and with Africa in particular. Amongst others, these included "harness(ing) India's experience with digital revolution to support Africa's development; improv(ing) delivery of public services; extend(ing) education and health; spread(ing) digital literacy; expand(ing) financial inclusion; and mainstream(ing) the marginalised" and "keeping our cyberspace safe and secure."

A sample of the memoranda of understanding (MoU) that has been signed with African countries elaborates on the type of ongoing cooperation (MEITY, n.d-a):

> "The MoU intends to foster active cooperation and exchange of knowledge and best practices between private entities, institutions involved in enhancing Capacity building, Governments and other public and private organisations of the two countries in the field of ICT. The main areas of cooperation are e-Governance, e-commerce, HRD and Capacity building in the ICT sector, electronics hardware manufacturing, Information Security etc (MEITY, n.d-b)."

ICT projects that have been undertaken in different countries in Africa include the Indo-Ghana Kofi Annan Centre of Excellence for Communications and Information Technology (CoEICT) at Accra, a Centre of Excellence for Communications and Information Technology (CoEICT) at Dar-es-Salaam, Tanzania and the India-Lesotho Centre of Excellence in ICT (ISCEICT) at Maseru, Lesotho (MEITY, n.d-c). The Indian Technical and Economic Cooperation Programme (ITEC) the flagship bilateral assistance program has recently started to offer short-duration technical programs in cyber technologies with the 2018 session offering courses at the Centre for Development of Advanced Computing (C-DAC), Pune and the Indian Institute of Technology, Kanpur (MEA, n.d). Earlier sessions in 2016 and 2015 had a few courses on cybercrime and cyber forensics conducted by Bureau of Police Research and Development (MEA, 2017). The ITEC programme sees 5,000 odd participants from Africa every year, so this is a major avenue for

co-operation (Economic Times, 2015). Indian digital initiatives like Aadhaar have been advocated by many as a solution to Africa's many problems, with some going to the extent of saying Africa would benefit more from Aadhaar than Chinese investments (Minter, 2018). The Indian Government has made sporadic efforts to promote Aadhaar elsewhere, but the consensus is that considering the sensitivities involved with cyber technologies, it is better to have countries approach India rather than the other way around (Raj and Jain, 2016).

6. Conclusion

A large number of users, the intrinsic lack of security architecture, and the global nature of cyberspace absent borders make the threat landscape much too large to be stabilised through traditional methods of mitigating threats such as effective law enforcement, and controls and regulations on the civilian side. The complexity and multi-layered nature of cyberspace also make international co-operation difficult to achieve, nonetheless, it has to be persisted with, in the absence of any alternative. Capacity-building efforts need to be expanded so that less developed countries can ramp up their defences against the digital threats. There is much scope for South-South cooperation since any developing countries also possess advance digital capabilities. The propensity of states to turn to the militarization of cyberspace as a fallback option to ensure that they have some means of securing their portion of cyberspace by building up offensive capabilities to deter any unwarranted actions by hostile actors is leading to a mutually reinforcing escalatory chain with no end in sight as new technologies bring new options and capabilities to the fore. With the current trajectory, states and their actions and inactions will be the main source of threats to the digital world unless urgent corrective action is taken.

References

Braw, Elisabeth, and Gary Brown. 2020. "Personalised Deterrence of Cyber Aggression." *RUSI Journal* 165 (2): 48–54.

Chappell, Bill (2017, 27 June). "'Petya' Ransomware Hits At Least 65 Countries; Microsoft Traces It to Tax Software." NPR, National Public

Radio, www.npr.org/sections/thetwo-way/2017/ 06/28/534679950/petya-ransomware-hits-at-least-65-countries-microsoft-traces-it-to-tax-software.

CIO East Africa (2017, 18 May) "ICT CS Joe Mucheru Calls for Information Sharing and Reporting on Cyber-Security Breaches.", www.cio.co.ke/news/ict-cs-joe-mucheru-calls-for-information-sharing-and-reporting-on-cyber-security-breaches-2/

Department of Homeland Security (n.d.), National Initiative for Cybersecurity Careers and Studies, "Explore Terms: A Glossary of Common Cybersecurity Terminology" ND. http://niccs.us-cert.gov/glossary

Global Forum on Cyber Expertise, (2017, March 16), *Cyber Crime and Cybersecurity Trends in Africa Report*.", p. 20 www.thegfce.com/documents/publications/2017/03/10/report-cyber-trends-in-africa.

ITU (n.d.), Definition of Cybersecurity, https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Livemint, (2016, July 8) "Aadhaar Goes Global, Finds Takers in Russia and Africa.", www.livemint.com/Politics/ UEQ9o8Eo8RiaAa NN My L b EK/Aadhaar-goes-global-finds-takers-in-Russia-and-Africa.html.

Ministry of Electronics and Information Technology (n.d-a), Active MoUs", Government of India, meity.gov.in/content/active-mous.

Ministry of Electronics and Information Technology (n.d-b), "International co-operation, Countrywise status| Ministry of Electronics and Information Technology, Government of India.", Government of India, meity.gov.in/content/country-wise-status

Ministry of Electronics and Information Technology (n.d-c), "International ICT Projects, Government of India, meity.gov.in/ content/international-ict-projects

Ministry of External Affairs (2017) "Civilian Training Programme, Indian Technical & Economic Cooperation (ITEC) 2016-2017." The Indian Technical and Economic Cooperation Programme (ITEC), www.itecgoi.in/downloads/2016-2017.pdf

Ministry of External Affairs (n.d.), ITEC Program. Available online at https://www.itecgoi.in/index.php

Minter, Adam. (2018, October 7) How India Could Transform Africa, Bloomberg, www.bloomberg.com/view/articles/2018-10-07/india-s-aadhaar-could-unlock-economic-growth-in-africa.

Mueller, Milton. Internet Governance Project "Threat Analysis of the WCIT Part 4: The ITU and Cybersecurity.", 20 Nov. 2017, www.internetgovernance.org/2012/06/21/threat-analysis-of-the-wcit-4-cybersecurity/.

Nye, Joseph S (2014, November). The Regime Complex for Managing Global Cyber Activities. Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, November 2014.

Saul, Jonathan (2017, June 29). "Global Shipping Feels Fallout from Maersk Cyber Attack." Reuters, Thomson, www.reuters.com/ article/ us-cyber-attack-maersk/global-shipping-feels-fallout-from-maersk-cyber-attack-idUSKBN19K2LE.

Signé, Landry, and Kevin Signé (2018, June 4). "Global Cybercrimes and Weak Cybersecurity Threaten Businesses in Africa." Brookings, Brookings, www.brookings.edu/blog/africa-in-focus/2018 /05/30/ global-cybercrimes-and-weak-cybersecurity-threaten-businesses-in-africa.

The Economic Times (2015, November 30), "Benefits for Africa as India Expands ITEC Programme.", economictimes.indiatimes.com/ news/economy/foreign-trade/benefits-for-africa-as-india-expands-itec-programme/articleshow/49982822.cms

The Spamhaus Project (n.d.), The Top 10 Worst Botnet Countries.", www.spamhaus.org/statistics/botnet-cc/.

United Nations (2010, July 30), "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.",

United Nations (2005, August 5), Report of the Secretary General, Submitted by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security https://disarmament-library.un.org/

United Nations (2018a, 22 December), *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. Resolution Adopted by the General Assembly on 22 December 2018, https://undocs.org/en/A/RES/73/266.

United Nations (2018b, 22 December), *Developments in the field of information and telecommunications in the context of international security*. Resolution Adopted by the General Assembly on 22 December 2018, https://undocs.org/en/A/RES/73/27