Research Report | XXVIII Annual Session

Special Conference 1

Measures to counter cyber security attacks and establishing cyber security strategies in the digital age

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Clara Babic

Forum:	Special Conference 1
Issue:	Measures to counter cyber security attacks and establishing cyber security strategies in the digital age
Student Officer:	Clara Babic
Position:	Deputy President

Introduction

As technology continues to evolve, so do the opportunities but also challenges that it presents. Today, we find ourselves at a crossroads moving from a society already entwined with the Internet to the coming age of automation, Big Data, and the Internet of Things (IoT). According to the International Telecommunications Union (ITU), a United Nations body for information and communication technologies (ICTs), as of 2017 almost 3.6 billion people are using the Internet, of which 2.6 billion are from developing countries. The total number of mobile phone users worldwide is forecast to reach around 4.7 billion in 2019, and the number of TV households worldwide around 1.7 billion in 2021. The truth is, in this modern world, in the digital age, it is impossible to walk down the street, sit on a train or even eat at a restaurant without being surrounded by people with eyes fixed on their smartphones, tablets or laptops. Simply think about spending a day without any of these items: your phone, the Internet, your TV, your car. A large number of people simply can't, and that is because technology has helped our lives become infinitely easier and overall better. As a result, we have become extremely dependent on it.

Just as technology brings ever-greater benefits, it also brings ever-greater threats: by the very nature of the opportunities it presents it becomes a focal point for cybercrime, industrial espionage, and cyber attacks. Therefore, protecting it is extremely important. Protecting that upon which we depend should be a priority for governments, businesses and industries, academia and every person with a smartphone in their pocket. Because, despite the quite technical name that it was given, the issue of cyber security is as vital to our way of life as technology itself. In fact, they cannot be separated: our economic health, our national security, and indeed the fabric of our society is now defined by the technology we use every day. Consider the connected devices the average person currently owns- smartphone, smart-TV, smart cars (as said previously), but now recognize that each one of them comes with vulnerabilities, making even you susceptible to an attack. Now, let's imagine these devices aren't just used to check emails or to turn on home security systems but are instead used to help treat or monitor a serious health condition, like Bluetooth-enabled defibrillators. The possibility of these devices being hacked is bigger than anyone ever thought, so a hacker could quite easily manipulate a defibrillator to deliver random shocks to a patient's heart or prevent a medically needed shock from occurring. Cyber security is also immensely important for governments, military, corporate, financial (and, as said previously, medical) organizations. Indeed, they collect, process, and stored unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information.

Definition of Key Terms

Internet

Essentially, the Internet is a global network of computing resources. By 1985, it was already well established as a technology supporting a broad community of researchers and developers and was beginning to be used by other communities for daily computer communications. Today, according to the ITU, more than 3.6 billion people use it. However, mostly in developing countries, some people still don't have access to the Internet, that is either because of a lack of infrastructure or affordability issues.

Digital age

Often also referred to as the Information age, or the Computer age, this concept reflects the ubiquitous nature of computing and the proliferation of technology in almost all aspects of human activity, such that digital interaction becomes a defining characteristic of said human activity. However, with our ever-increasing reliance on information and communication technology, we have witnessed the rise of more and more complex and sophisticated cyber-attack techniques. The degree of cyber threats has become more alarming, which is what we will see later on.

Cyber security

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.

Cyber security attacks / Cyber attacks

Cyber security attacks are considered deliberate exploitation of computer systems, technology-dependent enterprises and networks. Also known as cyber attacks, they use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.

Cyber security strategies

These strategies are designed to prevent and limit the number of cyber security attacks and breaches and improve the security and resilience of infrastructures and services. This consists of a wide variety of methods to be discussed later.

Internet of Things

Simply put, it's a collection of objects armed with sensors, which can produce data and transmit it over a communications network to each other and to the servers that control the sensors and do the data collecting. How does this impact you? Say for example, what if your alarm wakes you up at 6 a.m. and then notifies your coffee machine to start making coffee for you? That is an example of this concept, of basically connecting any device to the Internet or to each other. However, while they may lead to more efficiency in our daily lives, such connected devices run the risk of spying or hacking and leaving their consumers exposed to many dangers, ranging from disclosure of private information to problems with the devices themselves.

Big Data

Big Data refers to the large volume of data, which can be structured or unstructured, that organizations can analyse for insights that might lead to better business gains. However, as with the IoT, although it has many benefits, Big Data is also one of the most potentially destructive new technologies to come about in the last century.

Crypto-currency

Crypto-currency is a type of digital currency that uses cryptography for security and anti-counterfeiting measures (e.g. Bitcoin). They are quite highly risky because they are generally not backed by any tangible assets do not therefore offer any legal protection to consumers.

Cybercriminals

Cybercriminals are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit.

General Overview

As the so-called digital age continues to advance, more and more of our lives and assets comprise a growing digital element. Consider that a mere two hundred years ago our interactions were always physical, either in person or via written material, and our assets significantly measured in terms of their physical characteristics. Today, an increasing proportion of what we consider of value has taken a shape that can no longer be measured in physical terms, but only in digital terms. This could be as fundamental as our identity, for example, how we present ourselves to others via digital channels like Twitter or Instagram. We now interact with each other largely in digital ways, such as via Skype or Whatsapp. Our assets are now recorded digitally, such as the money we keep in the bank, our investment in stock markets, or even crypto-currency. ICTs now provide for a basis for all social, economic and cultural activities, as it has become more widespread and advanced, and its use and application has evolved. Arising from advancements in this field, cyberspace has thus become a crucial platform to promote national growth. The compelling pace at which this transition has been happening has overwhelmed governments. Once stable and relying on the traditional definitions of rights and duties, governments have been struggling to catch up on what exactly civic rights and duties mean or should mean in a digital era, providing the legal framework on which we can live our increasingly digital lives.

The struggle of government has also presented a major opportunity for unscrupulous people to leverage disconcerted authorities and wreak havoc in the parts of our lives that touch on the digital. So-called cybercriminals take advantage of ill protected digital assets (including physical assets that also have a digital footprint) by stealing, manipulating, destroying, or otherwise taking unauthorized advantage of them. Assets could be private or public. They could be as simple as an individual's personal email account, or as complex as the operation of an entire nation’s nuclear energy program. The consequences of cyber crime could be significant to individuals, such as destroying a person’s private life by revealing secrets. Or it could also be of significant detriment to vast amounts of people, such as when cyber criminals can potentially cause the electric grid to fail in an entire region, or change the outcome of a national election. The UN claim cyber crime produces as much as $1.5M trillion in revenue to criminals every year (UN News, 2018). As the digital world continues to extend, and as more and more technology continues to seep into our lives, governments face a huge challenge. They need to continue to protect citizens from cyber threats. The challenge lies in that the shape of digital assets continues to evolve at a very fast pace. Hence, the ways of protecting such assets needs to continue to evolve at least as fast. The challenge is compounded when one considers that with today’s high degree of connectivity, cyber criminals could well perpetrate crimes instantly affecting systems and people halfway across the world from the convenience of their couch. This not only makes detection harder, but when criminals work from one country to perpetrate crimes in another country, not much can be done to fight them without due international collaboration. Combating cyber crime seems to require at least as sophisticated an approach as combating regular crime, and governments are best armed to do it when considering cyber crime holistically and with all its facets.

Fighting cybercrime holistically means that it has to be done in the different contexts where it exists. Since it may occur at the local, national or international levels, it has to be fought at those instances. Investigating, prosecuting and adjudicating criminals requires proper legal frameworks in place that actually criminalize negative cyber activities in every jurisdiction, and these legal frameworks must be capable of rapidly evolving as new threats and modes of criminal activities are detected. At the same time, detecting and prosecuting these criminals requires a comprehensive operational capability that needs to be built and advanced continuously. Fighting cybercrime holistically also means that the different stages of crime must be considered. Significantly, this refers to efforts not only of investigating and prosecuting criminals ex post, but also to efforts in the prevention of crime. The prevention of crime in itself comprises many and various areas of consideration, including understanding what leads to the formation of cybercriminals and cybercriminal organizations, but also the very meaningful process of protecting the assets and the individuals and organizations that own these assets, which represent targets for cybercriminals. This starts with education. Just as we have been educated since we were children to lock the doors and windows of our house, or to leave our valuable assets properly secured when not in our direct control, we need to be trained to likewise secure our digital assets, whether at the organizational or individual levels, to help prevent cybercrime.

Governments have a key responsibility and must play multiple roles in combating cybercrime. This includes roles naturally matching the different branches of government, such as legislative, executive and judiciary. The legislative or regulatory ensures that the legal framework criminalizes cyber activity acting in detriment of the rights and duties of individuals and organizations. The executive operates to understand the causes of cyber crime, to prevent and detect it, and to prosecute criminals. The judiciary sees to it that criminals get adequate punishment and not commit crimes again. Given that cyber activity is no longer constrained to national borders, multilateral organizations, such as the United Nations, also have a key role to play. For one, cyber crime has prospered largely unchecked in countries with weak or improper regulation and with insufficient cyber capacity in the part of authorities. "A global effort is needed to provide better protection and firmer regulations because so far cyber criminals have hidden within legal loopholes in countries with less regulation" (UNIS, 2015). The United Nations, through its Office on Drugs and Crime (UNODC), supports national-level action and structures in the form of capacity building and in the establishment, dissemination and implementation of best practice in combating cybercrime. In a significant way, the private and business sector also has a fundamental role to play. First, segments in the business sector are the providers of most of the tools used to protect the targets of cybercrime at the individual and commercial levels. In building a business around cybercrime, they have self-adjudicated the onus of building the right tools to protect their customers from such crime, which they must honour. Second, the rest of the business sector itself is a significant target of cybercriminals. And just like all individuals must exercise caution and best effort to protect their assets, so must businesses.

Major Parties Involved

Russian Federation

The Russian Federation has been a key actor in the international arena in discussions to criminalize the misuse of information technologies since as early as 1998. It has also played a significant role in different UN-mandated organizations, such as the Group of Governmental Experts (GGE), as well as other multilateral organizations in trying to establish regulation at the international level. For instance, along with China and as part of the Shanghai Cooperation Organization, Russia proposed the Code of Conduct for Information Security in 2011. As evidenced recently, Russia's approach to cyber security, critical in fighting crime, is fundamentally different from that of the USA and other international actors, diverging significantly in their positions regarding freedom of flow of information, and the role of the state in regulating digital freedom (Giles, 2012). Russia has also been accused of carrying out massive cyber attacks against other nations (such as an alleged attack in Ukraine that neutralized much of the country's electric grid in 2015) and, while these claims remain unproven, it makes international consensus more complicated.

The United States of America

Arguably the most advanced global state in terms of its capability, power and reach, the USA have also played a significant role in trying to define cyber security policy globally. Domestically, several organizations are tasked with cyber security, including the cyber security arm at the FBI, as well as multiple computer crime units at the level of local or state law enforcement organizations. More relevant at the international level, the US Cyber security Command (part of the Department of Defense) has recently been elevated to a so-called Unified Combatant Command, effectively making it part of the USA's offensive weapon operations and systems. The power and extent of the USA's cyber security came to light significantly following the revelations of Edward Snowden, as well as the research carried out by other international cyber security teams, which point to the USA as the power allegedly behind some of the world's most sophisticated cyber security attacks in history (e.g., the development of Stuxnet to stall or neutralize Iran's nuclear program).

People's Republic of China

The Chinese government has been a collaborator and participant in international discussions to understand and regulate cyber crime since the early 90's. Probably its most fundamental contribution, along with Russia, has been that of the International Code of Conduct for Information Security, which was proposed by China and the rest of the Shanghai Cooperation Organization to the UN. China's views on freedom of flow of information is well known, tending to view control of information as one of the key roles of the state (significantly differing from the positions of other world powers, such as the USA). The most significant development, however, has happened domestically, with the new Cyber security Law coming into effect in June, 2017 (KPMG, 2017). Prior to this law, China already had some preliminary laws regulating cyberspace. However, the new law is significantly more comprehensive, and is also widely seen as evidence of China's increased focus on cyber security. Key considerations comprised in the Cyber security Law include protection of personal information, security of network operations and critical infrastructure, restrictions on information overseas and clear penalties for violating the law.

Brazil

As globalization drives Brazilian industries forward, it also invites threats that aim on the weaknesses of growing market economies. Financial crimes have always topped the list of cyber security issues in Brazil, but as the country's economy grows more people are exposed to the perks and problems of the latest computing technologies. Today, Brazil sends out the most number of spammed messages in Latin America. Almost two out of five (38%) malicious emails from the region come from Brazil. In addition, majority (58%) of malicious URLs are also hosted in Brazil. Increasingly learning from their counterparts in Eastern Europe via underground forums, Brazil could be considered as “an emerging cybercrime economy.”

Nigeria

The Nigerian Communications Commission (NCC) says Nigeria currently ranks third globally in cybercrimes behind the UK and the U.S. Committed mostly by the young, the often-called “Yahoo” boys are increasingly taking advantage of the rise in online transactions, electronic shopping, e-commerce and the electronic messaging systems to engage in heinous crime. The Central Bank of Nigeria (CBN) reported in 2015 that 70 per cent of attempted or successful fraud/forgery cases in the Nigerian banking system were perpetrated via the electronic channels. That same year, the Cybercrimes Act was passed into law to address the challenges. The law criminalizes a variety of offences – from ATM card skimming to identity theft. It imposes, for instance, seven years imprisonment for offenders of all kinds and additional seven years for online crimes that result in physical harm, and life imprisonment for those that lead to death. But like almost every law in the country, there is the problem of enforcement.

Vietnam

Vietnam's cyber security has been ranked 101st out of 195 countries in the Global Security Index of 2017 compiled by the ITU, while bordering nations Singapore, Malaysia and Thailand made it into the top 20. More than half of Vietnam's population (around 46 million) has access to the Internet. However, they are more prone to being harmed by it than many people around the world. In August 2016, Vietnam was the victim of cyber attacks on its two main airports. The Vietnamese government then vowed to fight against any form of cyber attacks on organizations or individuals, stating that all cyber attacks or threats to cyber security were to be condemned and severely punished in accordance with regulations and laws.

European Commission

The European Commission has been a significant player in the international arena through its individual member states, rather than as a unified group. The European Commission has been driving towards enhanced cyber security and so-called cyber resilience since the establishment of ENISA (European Union Agency for Network and Information Security) in 2005. However, its most significant joint effort sits at the European Cybercrime Centre, part of Europol, and is tasked with coordinating EU cross-border law enforcement activities related to cyberspace, and also serves as a key competence and skill centre in the area of cyber security. Much of the emphasis in Europe in relation to cyber security has been around the issues of privacy, and in trying to drive towards a so-called single digital market (the digital equivalent of a single “physical” market). A recent significant development in cyberspace in the EU has been the implementation of General Data Protection Regulation in 2018, which significantly enhances the rights of citizens to control their personal information (and severely limits what third parties can do with citizens’ personal information without their express authorization).

International Telecommunication Union

The International Telecommunication Union (ITU) is the largest UN-mandated organization responsible for issues related to information and communication technologies. The most significant contribution of the ITU has been the running of the World Conference on International Telecommunications (WCIT), which meets on an annual basis and has been responsible to develop proposals and fuel discussions of the International Telecommunications Regulations (ITRs), which “serve as the binding global treaty designed to facilitate international interconnection and interoperability of information and communication services, as well as ensuring their efficiency and widespread public usefulness and availability” (WCIT-12).

United Nations Group of Governmental Experts (UN GGE)

The Group of Governmental Experts (GGE) on information security is a UN-mandated group in the field of information security. As early as 1998 discussions started at the UN to move towards a consensus on a global cyber security agenda, and to discuss whether international law applies to the digital space. Since 2004, five working groups were established. After years of study the group concluded that “international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment, that voluntary and non-binding norms, rules and principles of responsible behaviour of States in the use of information and communications technologies can reduce risks to international peace” (UN, 2015, p2). The GGE is widely credited with “outlining the global cyber security agenda, and introducing the principle that international law applies to the digital space”. More recently, however, the fifth edition of the GGE failed to gain consensus on how states should behave in cyberspace, and therefore did not submit a report to the UN’s General Assembly, making the future of the group now uncertain (DigitalWatch, 2017).

Timeline of Key Events

Date	Description of Event
2013 - 2018	A gang of hackers, known as Carbanak, has, for the last five years, been targeting banks in at least 30 countries worldwide, stealing well over $1 billion in total. The gang targeted financial transfers and ATM networks from late 2013 by using a series of malware attacks (so, designed to damage or block computers) called Anunak and Carbanak. Following a coordinated international investigation, the (still anonymous) leader of the gang was caught in Spain.
November 21, 2017	The famous ridesharing app Uber releases a statement, revealing that hackers in 2016 stole personal information from around 57 million Uber users around the world, including their names and driver's license numbers, rider names, email addresses and mobile phone numbers. However, the story does not end here. The company admitted to having paid the hackers $100,000 to delete the stolen data and keep the breach quite, thus not reporting the incident.
July 17, 2017	Established by the United Nations in 2004, the Group of Governmental Experts (UN GGE) aimed to strengthen the security of ICTs. Up until now, the UN GEE has held five sessions, two of which have resulted in consensus reports. However, in 2017, they failed to present a much-anticipated fifth report, not being able to reach a consensus on whether or not international humanitarian law applied to cyber operations.
March 20, 2016	Malicious messages first hit Hillary Clinton's presidential campaign. Within nine days, some of its most consequential secrets were in the hackers' hands, who consequently tried to compromise Clinton's inner circle and more than 130 party employees, supporters and contractors.
2016	While in negotiations to sell itself to Verizon, the once major Internet pioneer, Yahoo, uncovered two major data breaches (which happened around 2013-2014), knocking an estimated $350 million off its sale price. These breaches are said to have compromised personal information of all 3 billion of its accounts, which were hacked.
2013	Edward Snowden, former NSA contractor, now living in exile in Russia, leaks the biggest cache of top-secret documents to the media, like for example, details of extensive internet and phone surveillance by American intelligence.
January 10, 2012	Google shocks the security community by disclosing that it (amongst other companies) was hit by attacks that originated in China, with some targeting Gmail accounts of Chinese human rights activists. As a result, the Internet giant said it would stop censoring its Web results in China. Google ended up exiting the

Chinese market altogether.

December 9, 2011 The United Nations Economic and Social Council (ECOSOC) holds a Special Event on Cyber Security and Development, organized by the International Telecommunication Union (ITU), joined with the Department of Economic and Social Affairs (DESA).

February, 2010 Chelsea Manning, formerly known as Bradley Manning, passed to Wikileaks a series of documents: the Iraq and Afghan war logs, diplomatic cables, and Guantanamo Bay files. One of the most notable files is a video, showing a US helicopter crew laughing as they launched an air strike killing a dozen people in Baghdad in July, 2007. She was released on May 17, 2017, after having served nearly seven years of a 35-year sentence.

November 23, 2001 Budapest Convention on Cybercrime, which came into force on July 1, 2004, is the first international treaty, which seeks to address cybercrime by harmonizing national laws, increasing cooperation between countries, as well as improving investigative techniques.

1998 First resolution on cyber security submitted to the United Nations by the Russian Federation.

Previous Attempts to Resolve the Issue

Debates concerning cyberspace have been present in the General Assembly's first committee for more than a decade. Today, more than a dozen organizations are involved, such as the Organization for Security and Co-Operation in Europe (OSCE) or the ITU. Cybercrime notably became a hugely discussed topic at the United Nations between 1998 up until 2004, culminating in the Budapest Convention on Cybercrime coming into force, on July 1, 2004. We can further note that when there was support from China and the United States the emergence and sponsorship of resolutions increased significantly. In 2010, a Group of Governmental Experts (GGE), consisting of diplomats from various powerful member states, stated: "existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century". This was followed by Russia, along with China and as part of the Shanghai Cooperation Organization, proposing the Code of Conduct for Information Security in 2011. In October 2013 the UN approved a Russian proposal titled: "Development in the field of information and telecommunications in the context of international security", a draft intended to keep the Internet and mobile communications secure. More recently, however, the fifth edition of the GGE failed to gain consensus on how states should behave in cyberspace, and therefore did not submit a report to the UN's General Assembly, making the future of the group now uncertain.

Thus, there have been some efforts in different international forums to address the issue. In various UN groups, government experts have been convening these last years in an effort to achieve consensus and common understandings on the norms that apply with respect to cyber security. However, to date, these efforts have had a limited impact, and progress, if made, is very slow.

Possible Solutions

Cyber threats are emerging as a pressing global challenge facing the international community. In order for the whole world to coexist in cyberspace, but also share its benefits, it is essential to acknowledge the different values of each country to build mutual trust and be able to work together to counter these challenges. In general, to establish efficient cyber security strategies, it is crucial to consider the prevention, incident management as well as consequence management of cyber security attacks. Meaning that, the before, during and after stages of the attacks are essential and to be included in resolutions, in order for a strategy to be effective.

Being in the Special Conference 1, it will be important to keep in mind that, as cyber threats are growing in their severity, existing measures and initiatives will probably no longer be capable of responding to these widespread and globalized risks. Vulnerability of cyberspace to these threats may impede activities in cyberspace and hamper free flow of information. Therefore, in addition to the existing measures and initiatives, there should be a new mechanism based on enhanced international cooperation in order to appropriately address the risks associated with the revolution in information and communication technology. For this, the importance of organizations such as ITU and the promotion of initiatives for international cooperation and mutual assistance in cyber security should be emphasized upon. It is not unlikely that terrorists or states wanting to attack a particular state or business using cyber terrorism or cyber warfare will look for the weakest links in the global chain and hit wherever they can to harm their primary target. The creation of a global action strategic plan in that regard could then be seen as a priority. International standards and norms to be applied across the board by states, and mechanisms for information sharing and cooperation, must be put in place sooner rather than later.

Although absolute prevention of cyber-attacks would be ideal, it has become incredibly difficult, because of the expansion of cyberspace as well as the sophistication of cyber threats. A more realistic approach is urgently needed. We already know that certain risks will occur and trigger incidents, but what is essential is a fast recovery from such incidents to mitigate any further damage that they might cause. One of the most pressing tasks for the international community is thus establishing a mechanism to implement a risk-based approach, where risks would be quickly and appropriately identified as they evolve and responded to dynamically. As stated before, absolute prevention of cyber-attacks is nearly impossible, however each government should still invest in having a reliable, real-time cyber security mechanism dealing with the identification of cyber threats likely to occur, and routinely checking information infrastructures for any signs of cyber activity that is suspicious. Systematic routine checks can thus be successful as prevention methods to avoid cyber security attacks (although not unilaterally).

In addition, although technology is the means through which cyber security attacks are carried out, it could also be a part of its solutions. Developments in technology may well provide solutions to the flaws of information infrastructure. It is, therefore, practical option to invest into research concerning technology to counter cybercrime. However, this would involve money and infrastructure that may not be available to developing countries. Thus, in order to address the mounting cyber challenges ahead, weaker states, whether NATO members or not, will need assistance in building up their capabilities. Domestic standards, laws, and institutions for combating cybercrime, cyber terrorism and cyber warfare will need to be put in place. International legal parameters will need to be defined and significant mechanisms for information sharing and cooperation will need to be created. Although this will not be easy, as there will likely be an amount of political opposition from states, and because of the diametrically opposed views from the United States and other Western countries, on one hand, and Russia and China on the other, regarding how cyberspace should be regulated; a concentrated effort is needed to try and close this serious gap in security.

Finally, in the age of globalization not only is it necessary to create the norms and infrastructure for states to work together to combat cross-border issues, but it may also be more possible to persuade states to do so if a strong lead is taken, whether by one powerful state or a group of states. Compelling measures must be put in place making it in the direct interests of states and industry to cooperate and adopt standards and cooperation methodologies. Aside from that, education on the subject that is cybercrime, as with any issue rising on the international front, is hugely needed. The lack of valid information of what actually constitutes cybercrime can be potentially dangerous because much of the fear arousing is from speculation on what it constitutes. Educating people on what they can do to protect themselves from cyber-attacks, amongst other things, is thus vital.

As cyber terrorism, cybercrime and cyber warfare pose a real and significant threat to national security. Together with increasing domestic efforts, strong operation on the international front is key.

Bibliography

Alexander, Harriet. “ Who is Chelsea Manning and why is she being released from prison?” Telegraph News and Media. 17 May, 2017. Web. 19 June 2018. <https://www.telegraph.co.uk/news/2017/05/17/chelsea-manning-released-prison/>

Associated Press, Bloomberg. “Inside Story: How Russians Hacked the Democrats' Emails”. Bloomberg News and Media. 3 Nov. 2017. Web. 19 June 2018. <https://www.bloomberg.com/news/articles/2017-11-03/inside-story-how-russians-hacked-the-democrats-emails>

Ayoub, Raddad; Firth, Clinton; Nayaz, Mohamed. “Cyber resilience in the digital age”. World Government Summit. https://www.worldgovernmentsummit.org/api/publications/document?id=24717dc4-e97c-6578-b2f8-ff0000a7ddb6

Christensson, Per. "Internet Definition." *TechTerms*. Sharpened Productions, 17 September 2015. Web. 9 July 2018. <https://techterms.com/definition/internet>.

Drozhzhin, Alex. "The greatest heist of the century: hackers stole $1 bln." *Computerworld Electronic Library Article. (2015). Web.* 19 June 2018. <*https://blog. kaspersky. com/billion-dollar-apt-carbanak/>*

Goldman, Jeff. “Carbanak Hackers Steal $1 Billion from 100 Banks Worldwide”. eSecurity Planet. 17 February, 2015. Web. 19 June 2018. <https://www.esecurityplanet.com/hackers/carbanak-hackers-steal-1-billion-from-100-banks-worldwide.html>

Hern, Alex. “Bitcoin and cryptocurrencies – what digital money really means for our future”. 29 Jan. 2018. The Guardian News and Media. Web. 20 June 2018. https://www.theguardian.com/technology/2018/jan/29/cryptocurrencies-bitcoin-blockchain-what-they-really-mean-for-our-future

Kaplan, Fred. “Obama Was Right to Commute Chelsea Manning’s Sentence”. Slate. 18 Jan. 2017. Web. 19 June 2018. <http://www.slate.com/articles/news_and_politics/war_stories/2017/01/why_president_obama_was_right_to_grant_chelsea_manning_clemency.html?via=gdpr-consent”

Khosrowshahi, Dara, “2016 Data Security Incident”. Uber Newsroom. Web. 19 June 2018. <https://www.uber.com/newsroom/2016-data-incident>

Lord, Nate, “What is Cyber Security?” 6 Apr. 2018. Digital Guardian. Web. 20 June 2018. <https://digitalguardian.com/blog/what-cyber-security>

Maurer, Tim. "Cyber norm emergence at the United Nations—an analysis of the UN’s activities regarding cyber-security." *Belfer Center for Science and International Affairs* 6668 (2011). 21 June 2018. <https://www.belfercenter.org/sites/default/files/files/publication/maurer-cyber-norm-dp-2011-11-final.pdf>

Marr, Bernard. “Why is Big Data so dangerous?”. Data Science Central. 14 Sep. 2016. Web. 9 July 2018. < https://www.datasciencecentral.com/profiles/blogs/why-is-big-data-so-dangerous>

MIT Technology Review Insights. “Cybersecurity in the Age of Digital Transformation” (2017). < https://www.technologyreview.com/s/603426/cybersecurity-in-the-age-of-digital-transformation/>

Morgan, Jacob. "A Simple Explanation Of'The Internet Of Things'." *Retrieved November* 20 (2014): 2015. Web. 18 June 2018. <https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#4dc90611d091>

Rouse, Margaret. “Internet of Things”. *Iot Agenda.* June 2018. Web. 9 July 2018. <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>

Statista Staff. “**Number of mobile phone users worldwide from 2015 to 2020 (in billions)” Statista. (2015-2016).** Web. 17 June 2018. **<**https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/>

Statista Staff. “Number of TV households worldwide from 2010 to 2021 (in billions)” Statista. (2010-2015). Web. 17 June 2018. <https://www.statista.com/statistics/268695/number-of-tv-households-worldwide/>

Tagert, Adam C. "Cybersecurity challenges in developing nations." (2010). Web. 9 July 2018. <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1021&context=dissertations&usg=AFQjCN>

Väljataga, Ann. “Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly”. 1 Sep. 2017. CCDCOE. Web. 20 June 2018. <https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html>

Wolter, Detlev. "The UN Takes a Big Step Forward on Cybersecurity." *Arms Control Today* 43.7 (2013): 25. < https://search.proquest.com/openview/d1265b6625577311d6d2dd9856e0c58a/1?pq-origsite=gscholar&cbl=37049>

Wong, C. Julia. “Uber concealed massive hack that exposed data of 57m users and drivers”. The Guardian News and Media. 22 Nov. 2017. Web. 19 June 2018. <https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack>

UN Involvement

Special Event on Cyber Security and Development – *9 December 2011.* <http://www.un.org/en/ecosoc/cybersecurity/index.shtml>

Developments in the field of information and telecommunications in the context of international security. <https://www.un.org/disarmament/topics/informationsecurity/> <https://www.ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf>

.