UNITED AMBASSADORS MODEL UN CONFERENCE (UA-MUNC)

UNITED NATIONS OFFICE IN GENEVA, 17-20 April 2018

SECRETARY GENERAL REPORTS

United Ambassadors Model United Nations Conference

Security Council B (High School)

Distr: General
Date: 25 February 2018
Original: English

First Session
Agenda Item 5

Cybersecurity Challenges as a threat to international peace and security

Report of the UA-MUNC Secretary-General

Introduction

1. In 2016 cybercrime became the second most reported crime in the world[1]. In the same year, the World Economic Forum estimated that the economic cost of cybercrime would reach 3 trillion dollars[2]. It is forecasted that this cost would increase to 6 billion dollars by 2021 if no action is taken towards limiting the threats presented by cybercrime[3]. Cybersecurity challenges are not only threatening governmental institutions and data, they threaten all business companies around the world and every single internet user. Such effects are related to the theft of classified information from governments, profits and market data from business, and private information and IDs from normal users. With growing threats from harmful cyber activities, a problem arises as governments and institutions fail to develop a strategy for cybersecurity. According to the International Telecommunication Union, only 38% of governments have published a strategy to combat cyber threats and only 12% of the world governments are currently developing strategies[4]. Cyberspace has been recently used as a platform for all kinds of illicit trafficking including drugs, weapons, small arms, children, and cultural property[5]. Such challenges on cybersecurity are formed by cyber-attacks, viruses, worms, web hacking, cyber espionage, and E-commerce Fraud, etc.[6]. A key issue in the development of cybersecurity challenges is that it hinders progress

[1] 107 Cybersecurity & Cyber Crime Statistics, Facts + Studies (2017-2018) https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

[2] Morgan, S., 2017. Is cybercrime the greatest threat to every company in the world? *Cybersecurity Business Report*. Available at: Is cybercrime the greatest threat to every company in the world? [Accessed January 31, 2018].

[3] 107 Cybersecurity & Cyber Crime Statistics, Facts + Studies (2017-2018) https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

[4] Half of all countries aware but lacking national plan on cybersecurity, UN agency reports | UN News https://news.un.org/en/story/2017/07/560922-half-all-countries-aware-lacking-national-plan-cybersecurity-un-agency-reports#.WmSBEiOB2b9

[5] UNODC, 2017. Countering Illicit Arms Trafficking and its Links to Terrorism and Other Serious Crime UNODC's Global Firearms Programme. *UN*. Available at: https://www.un.org/sc/ctc/wp-content/uploads/2017/05/Simonetta-UNODC-at-CTED_May2017v2.pdf [Accessed January 31, 2018].

[6] USAID, Cyber Crime: Its Impact on Government, Society and the Prosecutor. *USAID*. Available at: http://pdf.usaid.gov/pdf_docs/Pnada641.pdf [Accessed January 31, 2018].

towards achieving the sustainable development goals, to be discussed later in this report.

Topic Background and History

The emergence of Information and Communications Technology (ICT)

2. The issue of cybersecurity and the challenges facing it dates back to the start of information technology in the 1940s. At the time, militaries were the only known organizations applying research and development towards the process of automation. Later, in the 1950s, the first commercial computer was launched which was called the UNIVAC I, created by John Eckert and John W. Mauchly. At the same time several computer generations were developed and each was for a different purpose. Since then computers have been used to do calculations, store data and information in databases, design air crafts and nuclear reactors, and predict weather forecasts. The term information technology emerged in the 1970s, which also saw the development of microcomputers by different organizations. After these technological developments, the term information technology was changed to Information and Communications Technology (ICT)[7].

The Beginning of the Internet

3. Another factor that helped in increasing the use of ICTs was the development of the internet. Given the magnitude of the invention, the development of the internet cannot be considered as the creation of a single person. However, it is the product of many studies and research conducted by several scientists throughout history. In the 1900s many scientists had a vision for the development of a world wireless system. However, the first practical version of the internet did not develop until the early 1960s. What followed was the development of the first effective method to transmit electronic data between computers. The first workable version of the internet was called the ARPANET and was funded by the U.S Department of Defense. In the 1990s, the first modern version of the internet was released by the computer scientist Tim Berners-Lee known as the "world wide web". In this web, online information and data were easily accessed in the form of websites and hyperlinks[8].

International Action

4. With the increase in the usage of the world wide web, several issues and threats started to appear as with every new invention that was created. The internet and the accompanying information and telecommunication devices and systems created a platform for theft and crime to happen through the web and the internet. Such threats alarmed governments and the international community particularly the UN. This in turn led to the start of the adoption of yearly resolutions by the GA since 1998 on the topic of Developments in Telecommunications and Information in the context of international security[9]. Moreover, the Council of Europe started to discuss the issues and to adopt declarations, plans, and Agendas to secure the world and the European

[7] NUS, 2008. History of ICT. *Wiki.nus*. Available at: https://wiki.nus.edu.sg/display/cs1105groupreports/History of ICT [Accessed February 2, 2018].

[8] Andrews, E., 2013. Who invented the internet? *History.com*. Available at: http://www.history.com/news/ask-history/who-invented-the-internet [Accessed February 2, 2018].

[9] United Nations, United Nations Official Document. *United Nations*. Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A%2FRES%2F53%2F70 [Accessed February 1, 2018].

Union[10]. Earlier, the issue of cybercrime was dealt with as a transnational crime because it was not tracked to a specific location or entity but rather in different locations and therefore, governments were not able to deal with such crimes in order to prosecute jurisdictions.

Development on Usage

5. As we entered the 21st century, ICTs and the internet are no longer a want, but a necessity of society. In 2017, the number of internet users worldwide reached 3.58 billion,[11] while the number of mobile users worldwide is 4.77 billion[12]. Those numbers show how much our modern world is becoming integrated into using technology and the internet. Thus, with such increases in the usage of ICT, incidents of cybercrime and cyber theft have become more frequent and are presenting greater threats to international security and the global community, including threats presented to normal internet users, banks and financial institutions, governments and classified data bases, businesses, and militaries[13].

Effects of Cybersecurity Challenges

Effects of Cybersecurity Challenges on Businesses

6. Cybersecurity challenges have been creating many obstacles for businesses worldwide. According to several studies, 85% of business data and information is stored on online platforms[14]. Additionally, according to Forbes it is predicted that cybercrime would cost businesses around the world $6 trillion by 2021[15]. Such cost increases for businesses starts with extremely high costs in developing systems and firewalls to protect businesses' and customers' sensitive data from breaches. Moreover, the costs are also represented by the losses that the firms make when there are breaches, and they lose the competitive advantage from their stolen plans or specifications. Furthermore, companies lose a significant value of their sales because customers start to lose trust in the firms because their personal information has been breached or because the company starts to lose the identity it built. In extreme cases the company is even sued by its own customers for the data and information that has been stolen and this makes it even more challenging for the firm to build trust with new customers. Lastly, companies spend a significant amount of money trying to build new strategies on how to store their data elsewhere to be safe from such attacks[16].

Effects on Governments and Militaries

7. The issue of securing data and establishing security measures to protect sensitive data and military weapons for governments could be challenging for various Member

[10] Council of Europe, Reports. *Cybercrime*. Available at: https://www.coe.int/en/web/cybercrime/all-reports [Accessed January 19, 2018].

[11] Statista, 2018. Number of internet users worldwide 2005-2017. *Statista*. Available at: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/ [Accessed February 3, 2018].

[12] Statista, 2018. Number of mobile phone users worldwide 2013-2019. *Statista*. Available at: https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/ [Accessed February 3, 2018].

[13] InfoSec Institute, 2015. 2013 - The Impact of Cybercrime. *InfoSec Resources*. Available at: http://resources.infosecinstitute.com/2013-impact-cybercrime/#gref [Accessed February 12, 2018].

[14] Veritas Global, 2018. News Release. *Veritas Global Databerg Report Finds 85% of Stored Data Is Either Dark, or Redundant, Obsolete, or Trivial (ROT)*. Available at: https://www.veritas.com/news-releases/2016-03-15-veritas-global-databerg-report-finds-85-percent-of-stored-data [Accessed February 1, 2018].

[15] Council, Y.E., 2017. The True Cost Of Cybercrime For Businesses. *Forbes*. Available at: https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#8d5109349476 [Accessed February 4, 2018].

[16] Clickatell, Cybercrime and its effect on businesses. *Clickatell*. Available at: https://www.clickatell.com/articles/information-security/cybercrime-effect-businesses/ [Accessed February 5, 2018].

States. Hacks or breaches of classified information can significantly harm governments because such information can be seen by the public or could be accessible to other Member States. This can have a negative effect on the government because it causes domestic disorder or protests, and distrust between the people and the government. Moreover, it can harm the international relations between Member States if the classified information relates to other international organizations. Therefore, the breaches in sensitive governmental information can harm the political and diplomatic position or stance of the targeted Member State[17].

8. Another major international issue is the protection of the automated release of weapons from cyber-attacks. For the most part, in instances where nations have possession of nuclear weapons or other ballistic missiles, these would be released through an automated technological system and therefore, they could be released if the system was hacked. The consequence of such an action could result in the death of millions, if not the complete destruction of nations or geographical areas. The reason why this is an issue is that nuclear weapons and several ballistic missiles were developed before the significant advancement of technology systems and cyberspace. Thus, the methods used by hackers and cyber breaches are more advanced than the systems placed to protect the weapons and monitor their condition. Since then, governments have been placing a significant amount of funds and efforts to improve their protection systems for weapons in order to secure their militaries from such attacks[18].

Cybersecurity and the SDGs

9. The development of cybersecurity measures and the use of ICTs can have a direct effect on the implementation of the Sustainable Development Goals (SDGs). Some of the SDGs directly linked to the issue of cybersecurity are goals 5, 9, 11, and 17. Achieving gender equality and the empowerment of girls and women (SDG 5) is linked to the availability of opportunities online for the women to receive education and find job opportunities and thus, the safety and the accessibility of cyberspace is linked to achieving this SDG for females[19]. Additionally, for SDG 9, the development of industries, innovation, and infrastructure is directly linked to the accessibility of a safe cyber network in order to allow for better management of infrastructure, maintenance, additional business opportunities, and online services[20]. SDG 11 to make cities more inclusive, safe, and sustainable, is also linked to limiting the cybersecurity challenges because such healthy technological programs can allow communication and detection of natural disasters to allow more proactive protection measures[21]. Moreover, SDG 17 which is about global partnership to reach sustainable development, could be reached by limiting the threats of cybersecurity on cyberspace because a secured cyberspace can ease the process of information sharing and connect people and institutions[22].

[17] Eggers, W.D., 2016. Government's cyber challenge: Protecting sensitive data for the public good. *Deloitte Insights*. Available at: https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/protecting-sensitive-data-government-cybersecurity.html [Accessed January 30, 2018].

[18] Ashford, W. ed., 2018. Nuclear weapons' cyber attack risk relatively high, says report. *ComputerWeekly*. Available at: http://www.computerweekly.com/news/450432994/Nuclear-weapons-cyber-attack-risk-relatively-high-says-report [Accessed February 14, 2018].

[19] ITU, 2018. Goal 5. Gender. *ITU*. Available at: https://www.itu.int/en/sustainable-world/Pages/goal5.aspx [Accessed February 11, 2018].

[20] ITU, 2018. Goal 9. Infrastructure, Industrialization, Innovation. *ITU*. Available at: https://www.itu.int/en/sustainable-world/Pages/goal9.aspx [Accessed February 11, 2018].

[21] ITU, 2018. Goal 11. Cities. *ITU*. Available at: https://www.itu.int/en/sustainable-world/Pages/goal11.aspx [Accessed February 11, 2018].

[22] ITU, 2018. Goal 17. Implementation. *ITU*. Available at: https://www.itu.int/en/sustainable-world/Pages/goal17.aspx [Accessed February 11, 2018]

Thus, the SDGs are directly impacted by the establishment of a safe cyberspace, and existing security challenges place several obstacles on achieving these goals.

Conflict with Human Rights

10. As governments have realized the significant effects of the threats to cybersecurity, they usually take measures to strengthen their cybersecurity systems and programs which decreases the possibility of cyber-attacks occurring. However, another issue appears which relates to the privacy of individuals on the internet and their right to acquire information online. Usually, governments start constricting access to several websites or data on the web in order to increase the security of the web. Moreover, they may have access to private accounts or personal histories on search engines or location signals in order to tract possible cyber threats or attacks. Even though such measures can limit the threats on cybersecurity, they breach a fundamental right of all individuals, which is the right to privacy and access to information. Additionally, in most cases, governments use the approach of securing the country's cyberspace in order to increase censorship and gain access to local data on the web and to hide classified information from the public. Thus, there is always a tradeoff between increasing cybersecurity measures and the right to privacy for cyberspace users. Lately, governments have been trying to find measures in which the right to privacy is not breached and at the same time, cyber space is secured; while others have been abusing this approach by adding more limitations on internet users and accessing more private information[23].

Committee Introduction

11. The Security Council is one of the six main organs of the United Nations and its first session took place on 17 January 1946. It is responsible for maintaining international peace and security and responding to any such threats. The Security Council has 15 members of which 5 are permanent, and 10 are nonpermanent and rotate every two years. Each month there is a different president from the different Member States participating in the Council and they are selected in alphabetical order. This UN organ is the only organ that has the power to pass legally binding resolutions which Member States have to carry out under article 25 of the UN Charter. For the voting procedure, each Member State in the council counts for one vote and the five permanent members of the council have the "veto" power. In order for a vote to pass it must pass by acclimation without any veto power voting against[24].

12. The mandate and the Jurisdiction of the council can be found in UN Charter Chapters VI and VII. Chapter VI aims at limiting threats or solving disputes by peaceful means such as setting principles for agreement, dispatch a mission, appointing envoys, or undertaking investigation and mediation. Chapter VII takes a more provisional measure to limit escalated threats, and include measures such as placing economic sanctions, cutting diplomatic relations, calling for collective military action to be led by the Department of Peacekeeping Operations whenever necessary under article 39

[23] Public Knowledge, 2018. Cybersecurity and Human Rights. *Public Knowledge*. Available at: https://www.publicknowledge.org/cybersecurity-and-human-rights [Accessed February 10, 2018].

[24] United Nations, 2018. Security Council, SC, UNSC, security, peace, sanctions, veto, resolution, president, united nations, UN, peacekeeping, peacebuilding, conflict resolution, prevention. *United Nations*. Available at: http://www.un.org/en/sc/about/ [Accessed February 14, 2018].

of the UN charter[25]. The Security Council has partnered with many international and regional organizations to improve their efficiency in the implementation of the decision taken such as the Council of Europe, Interpol, the International Telecommunications Union, and other non-governmental organizations[26].

Past International Action

Budapest Convention on Cyber Crime (2001):

13. This is the first international Convention to discuss the issue of cybercrime and protecting the use of the internet and ICTs, and was opened for signature in 2001 and came into force in 2004[27]. Originally it was launched by the Council of Europe and later on other nations outside Europe joined and therefore, it is not currently globally recognized because it still needs additional ratifications. As of December 2016, 52 Member States have ratified the convention and 4 other states are current signatories but have not yet ratified it[28]. The convention focuses on calling for international cooperation on the matter and encouraging Member States to set a domestic legal system to protect the usage of internet and ICTs, as well as to set a reasonable system for investigation and prosecution for cyberattacks. Moreover, the convention defined several terms related to the topic to be discussed later. The Convention is currently considered the primary source of information and international cooperation between nations on the issues of cybersecurity challenges. Governments regularly consider the convention when examining the issues of cyber threats and when aiming to implement strategies[29]. Therefore, this convention is considered the initial step in setting measures to limit existing Cybersecurity threats and has been followed up by several efforts such as the Additional Protocol on the Convention on Cybercrime, which was adopted by the Council of Europe Committee of Ministers on 7 November 2002. This additional Protocol was considered a milestone in combatting Racism and Xenophobia generally, and when cyberspace is used as a medium for such actions[30]. The Convention and its additional protocols are considered as successful progress in fighting cyber threats but require greater awareness, state ratifications, and implementation for it to become internationally recognized.

The General Assembly:

14. The General Assembly has been dealing with issue of cybersecurity by passing many resolutions and through holding several discussions during its sessions. The first resolution adopted by the GA on this topic was resolution 53/70[31]. This resolution highlighted the link between international security and information technology and

[25] United Nations, 2018. Security council, SC, UNSC, security, peace, sanctions, veto, resolution, president, united nations, UN, peacekeeping, peacebuilding, conflict resolution, prevention. *United Nations*. Available at: http://www.un.org/en/sc/about/functions.shtml [Accessed February 23, 2018].

[26] Security Council, 2007. Cooperation with International, Regional and Subregional Organizations | UN Counter-Terrorism Committee. *United Nations*. Available at: http://www.un.org/en/sc/ctc/cooperation.html [Accessed February 15, 2018].

[27] Council of Europe, 2018. Chart of signatures and ratifications of Treaty 185. *Council of Europe*. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures [Accessed February 22, 2018].

[28] Council of Europe, 2018. Chart of signatures and ratifications of Treaty 185. *Council of Europe*. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures [Accessed February 22, 2018].

[29] Global Forum on Cyber Expertise, 2016. The Budapest Convention on Cybercrime: a framework for capacity building. *Global Forum on Cyber Expertise*. Available at: https://www.thegfce.com/news/news/2016/12/07/budapest-convention-on-cybercrime [Accessed February 22, 2018].

[30] Council Of Europe, 2003. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. *Council Of Europe*. Available at: http://www.notohatespeech.com/wp-content/uploads/2016/08/AP-Cybercrime.pdf [Accessed January 21, 2018].

[31] United Nations, Resolution Adopted by the General Assembly. *United Nations*. Available at: https://undocs.org/A/RES/53/70 [Accessed January 31, 2018].

was adopted without a vote, i.e. it was adopted by consensus[32]. Moreover, this resolution requested the Secretary General to prepare a report on the topic and encouraged all states to cooperate in good faith to come up with international definitions to terms related to the topic. Later on, the GA passed resolution 58/32 in 2003, from which a Group of Governmental Experts (GGE) was created to cooperate with the Secretary General in preparing the report on the issue of cyber threats and measures to strengthen cybersecurity[33]. The use of the Group of Governmental Experts was considered an efficient tool for research on the issue of cyber threats and was later implemented several times with newer tasks through resolutions 68/243 and 70/237[34]. Resolution 68/167 adopted in 2013, focused on the issue of the right to privacy in the digital age. The resolution focused primarily on the importance of not breaching privacy rights while creating measures for cybersecurity[35]. Furthermore, the GA adopted resolution 69/28 in 2014, which called on states to work on developments in the field of information and telecommunication in relation to international security[36]. The GA has called on Member States to cooperate in information sharing and confidence building in relation to measures for cybersecurity. Moreover, they requested Member States to submit their opinions on existing international laws that related to the issue[37]. Thus, the General Assembly has demonstrated various efforts to deal with existing cyber threats and aid Member States in dealing with such issues however, the problem with such efforts is that they are all in the form of recommendations and possible solutions. Member States continue to ignore such solutions and approaches and refuse to cooperate and share information and capacity building measures on the issue at hand. Therefore, such recommendations will never make the global cyberspace secured until they are accompanied with immediate action.

The International Telecommunication Union (ITU):

15. This Agency under the United Nations focuses on topics related to information and communications and strongly addresses the issue of cybersecurity challenges. The primary purpose of this agency is to write reports and host summits. Along with report writing, the ITU makes recommendations to Member States on how to deal with emerging technological threats[38]. The World Summit on Information Societies (WSIS) is hosted by ITU and began in 2001. WSIS usually sets goals to be achieved to help limit cybersecurity challenges. Some of those goals were released in 2005 and are not limited to: expanding access to information, increasing capacity building and information sharing, emphasizing international and regional cooperation, and building international security measures for the use of ICTs[39]. Moreover, the ITU launched the Global Cybersecurity Agenda (GCA), a collaborative platform to aid cooperation and information sharing on the issue of cybersecurity while focusing on

[32] United Nations, Developments in the field of information and telecommunications in the context of international security – UNODA. *United Nations*. Available at: https://www.un.org/disarmament/topics/informationsecurity/ [Accessed February 11, 2018].

[33] United Nations, Resolution adopted by the General Assembly. *United Nations*. Available at: https://undocs.org/A/RES/58/32 [Accessed February 11, 2018].

[34] United Nations, Developments in the field of information and telecommunications in the context of international security – UNODA. *United Nations*. Available at: https://www.un.org/disarmament/topics/informationsecurity/ [Accessed February 11, 2018].

[35] United Nations, Resolution Adopted by the General Assembly. *United Nations*. Available at: http://undocs.org/A/RES/68/167 [Accessed February 14, 2018].

[36] United Nations, Resolution Adopted by the General Assembly. *United Nations*. Available at: https://undocs.org/A/RES/69/28 [Accessed February 15, 2018].

[38] United Nations, Overview. *ITU*. Available at: https://www.itu.int/en/about/Pages/overview.aspx [Accessed February 21, 2018].

[39] United Nations, World Summit on the Information Society (WSIS) .:. Sustainable Development Knowledge Platform. *United Nations*. Available at: https://sustainabledevelopment.un.org/index.php?page=view&type=30022&nr=102&menu=3170 [Accessed February 17, 2018].

five main pillars. The pillars of the GCA are international cooperation, organizational structures, capacity building, and technical and procedural measures. Thus, the GCA sets the main goals or areas on the issue of cybersecurity challenges. However, the GCA's work is guided by the High-Level Experts Group (HLEG), a group of experts on cybersecurity who work together to provide the information needed to the GCA[40]. Due to the fact that the SDGs are strongly related to cyber space and the use of ICTs, the ITU released a campaign with a hashtag called #ICT4SDG. This campaign works on raising awareness about the importance of both the SDGs and the use of ICTs and how they are strongly related by describing the effect of ICTs on the achievement of each of the SDGs[41]. Thus, with such diversity in the approach of raising awareness and dealing with cyber threats, the reach and progress of the ITU has been effective and efficient. Mostly, the summits, reports, and campaigns were the tools that made the governments and the general public aware of the issue, initiate action and, set Agendas to make their cyberspace more secure.

Member States:

16. Many Member States have started different initiatives to limit the threats of cybersecurity. States such as the United Kingdom and the United States have created domestic offices dedicated to combating cybersecurity challenges. For example, in the US, the Office of Cybersecurity and Communication (CS&C) is responsible for maintaining cybersecurity and focuses on securing important data that affects individuals, the government, and the economy. The office also collaborates with commercial websites in the US to ensure the safety of cyberspace for all users. An additional job of the Office, is to serve 24/7 and act on incident response and cyber monitoring[42]. Furthermore, in the UK, there is the National Cybersecurity Center which has a similar job to the CS&C[43]. Such offices are one of the many solutions that can help create a more protected and safe cyberspace and enable Member States to have control over the potential threats to cybersecurity.

Other Organizations

FIRST:

17. This is a computer security organization which focuses on initiating incident responses. The organization was created in 1990 as a response to previous attacks and worms which spread in cyber space at the time. With the increase in the usage of the internet and information, the organization continued to expand and develop their security teams. Membership of FIRST allows instant response to any cyber-attack through the internet or on ICTs, and as such, it increases the safety of the technology usage. Moreover, FIRST hosts several annual conferences in which propaganda is made about their services and in which alternative and advanced methods of instant response and protection are shared[44]. Lastly, organizations such as FIRST have a clear

[40] United Nations, Global Cybersecurity Agenda (GCA). *Global Cybersecurity Agenda (GCA)*. Available at: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx [Accessed February 12, 2018].
[41] United Nations, ICTs for a Sustainable World #ICT4SDG. *ICTs for a Sustainable World #ICT4SDG*. Available at: https://www.itu.int/en/sustainable-world/Pages/default.aspx [Accessed February 2, 2018].
[42] Department of Homeland Security, 2017. Office of Cybersecurity and Communications. *Department of Homeland Security*. Available at: https://www.dhs.gov/office-cybersecurity-and-communications [Accessed February 2, 2018].
[43] GOV.UK, Cyber and Government Security Directorate. *Cyber and Government Security Directorate - GOV.UK*. Available at: https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance [Accessed February 3, 2018].
[44] First, FIRST History. *FIRST - Forum of Incident Response and Security Teams*. Available at: https://www.first.org/about/history [Accessed February 15, 2018].

mission statement in which they show their determination to the protection of the internet and the usage of cyber technology[45].

Interpol:

18. Interpol is the world's largest international police organization with 192 member countries. The organization has an aim of enabling different domestic police organizations to cooperate efficiently to ensure the safety of individuals globally[46]. As a global security organization, Interpol has a significant role in addressing the threats of cybersecurity. Interpol focuses on fighting cybercrime generally, and any crime that is enabled through the use of cyberspace or cyber technologies. National partnerships with most cybersecurity offices are the main method used by Interpol to deal with the transnational nature of cybercrime in an effective and efficient manner. Through its different operations, Interpol provides Member States with operational and investigative support, cyber intelligence and analysis, innovation and research, capacity building, and national cyber reviews. With such diversity in its approaches, Interpol is an effective and active contributor and assistant to limit cybersecurity threats globally[47]. Another initiative by Interpol is the Global Complex for Innovation (ICGI). The ICGI is a facility located in Singapore for the identification of crimes and criminals with a high edge in research and development. The main aim of this facility is to give policy organizations worldwide the edge on criminals and to be able to act upon and access information within a relatively short period of time. Another goal of this Global Complex is to provide police organizations around the world with digital security, capacity building and training, and operational and investigative support. Such efforts are planned to help police organizations to deal with the fast and technological approach of cyber threats and crimes[48]. Thus, if such training and cooperation were efficient, then police organizations would be able to contribute to securing their nation's cyberspace.

Commonwealth Cyber Initiative:

19. The Commonwealth Cybercrime Initiative (CCI) is a multilateral forum that aims at reducing cybercrime and strengthening the measures for cybersecurity through increasing the sharing of information and cooperation between members of the commonwealth, and with other organizations and Member States. The CCI cooperates with around 35 international organizations such as Interpol, the Council of Europe, and the ITU. The main aim of the CCI is in assisting Member States to analyse the security of their cyberspace and recommend solutions to strengthen such securities. Analyses are usually made in the form of reports conducted by criminal justice and technical experts. Solutions are usually in the form of a set agenda suggested by the CCI and applied by the Member States. An example of the efforts of the CCI was a cooperative effort with the United Nations Office on Drugs and Crime (UNODC) in holding an assessment on the situation in Tanzania[49]. The CCI is thus facilitating more

[45] First, FIRST Vision and Mission Statement. *FIRST - Forum of Incident Response and Security Teams*. Available at: https://www.first.org/about/mission [Accessed February 15, 2018].

[46] Interpol, Overview. *Overview / About INTERPOL / Internet / Home - INTERPOL*. Available at: https://www.interpol.int/About-INTERPOL/Overview [Accessed February 23, 2018].

[47] Interpol, Cybercrime. *Cybercrime / Cybercrime / Crime areas / Internet / Home - INTERPOL*. Available at: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime [Accessed February 23, 2018].

[48] Interpol, The INTERPOL Global Complex for Innovation. *The INTERPOL Global Complex for Innovation / About INTERPOL / Internet / Home - INTERPOL*. Available at: https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation [Accessed February 23, 2018].

[49] Commonwealth, 2018. Commonwealth Cybercrime Initiative. *Commonwealth Cybercrime Initiative | The Commonwealth*. Available at: http://thecommonwealth.org/commonwealth-cybercrime-initiative [Accessed February 4, 2018].

efficient cooperation between organization to help guide Member States facing the threats of cybersecurity.

Terms Defined:

20. Some of the terms defined in the Budapest Convention on Cybercrime in 2001

Word	**Definition**
Computer System	Any device or a group on interconnected or related devices, one or more of which, pursuant to a program, preforms automatic processing of data[50]
Computer Data	Any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function[51]
Service Provider	Any public or private entity that provides to users of its service the ability to communicate by means of a computer system and any other entity that processes or stores computer data on behalf of such communication service or users of such service[52]
Traffic Data	Any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service[53]

21. Even though there are no agreed upon definitions by the Member States on the phrases related to the topic, the following dictionary definitions are necessary for the understanding of the topic

Word	**Definition**

[50] Council of Europe, Convention on Cybercrime. *Council of Europe*. Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [Accessed February 14, 2018].

[51] Council of Europe, Convention on Cybercrime. *Council of Europe*. Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [Accessed February 14, 2018].

[52] Council of Europe, Convention on Cybercrime. *Council of Europe*. Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [Accessed February 14, 2018].

[53] Council of Europe, Convention on Cybercrime. *Council of Europe*. Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [Accessed February 14, 2018].

Cyber Space	It is the notional environment in which communication over computer networks occur[54]
Cybersecurity	The state of being protected against the criminal or unauthorized use of electronic data or the measures taken to achieve this[55]
Cybercrime	Criminal activities carried out by means of computers or the internet[56]

Political Groups

The African Union (AU):

22. The African economy has been recently booming, and the use of ICTs and the internet has significantly increased. In 2000, only 4.5 million users in Africa were online, while in 2016 an estimated 300 million users are now online. Such an increase in the demand on ICs and the internet, required the African Union and its Member States to make efforts in placing the necessary legislations for the protection of their cyberspace and their users. The initial step was the passing of the Convention on Cybersecurity and Personal Data Protection by the AU in 2014. In this convention, there is a call for a continental legal framework for personal data protection, cybersecurity, and cybercrime. Moreover, it calls on all Member States to build an information society that values and respects the culture of the African Community[57]. However, the convention only has 10 signatories and 1 ratification from a total of 55 African Nations.[58] The reason why the convention does not yet have many signatories is due to the alarming fact that many of the African Nations still find the issue of cybersecurity threats irrelevant and also because other nations are waiting for more critiques and evaluations to be made about the convention. The AU is also currently working on the Draft of the African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa. The main aim of this convention would be to strengthen existing domestic legislations against cyber threats and to develop the necessary harmonization of legislations between the African Member States[59]. Furthermore, the AU has been making significant effort in capacity building measures through the workshops and summits held to discuss annual topics, while constantly aiming to build cooperation for a stable and secured digital African environment[60]. Thus, with such efforts from the AU, the African cyberspace will most likely become secured and the users would be protected from cyber threats in the upcoming years.

The European Union (EU):

[54] Dictionary.com, cyberspace. *Dictionary.com*. Available at: http://www.dictionary.com/browse/cyberspace?s=t [Accessed February 1, 2018].

[55] Dictionary.com, cybersecurity. *Dictionary.com*. Available at: http://www.dictionary.com/browse/cybersecurity?s=t [Accessed February 1, 2018].

[56] Dictionary.com, cybercrime . *Dictionary.com*. Available at: http://www.dictionary.com/browse/cybercrime?s=t [Accessed February 13, 2018].

[57] African Union, AFRICAN UNION CONVENTION ON CYBERSECURITY AND PERSONAL DATA PROTECTION. *African Union*. Available at: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf [Accessed February 18, 2018].

[58] African Union, AFRICAN UNION CONVENTION ON CYBERSECURITY AND PERSONAL DATA PROTECTION. *African Union*. Available at: https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection_1.pdf [Accessed February 19, 2018].

[59] African Union, DRAFT AFRICAN UNION CONVENTION ON THE ESTABLISHMENT OF A CREDIBLE LEGAL FRAMEWORK FOR CYBERSECURITY IN AFRICA. *DRAFT AFRICAN UNION CONVENTION ON THE ESTABLISHMENT OF A CREDIBLE LEGAL FRAMEWORK FOR CYBERSECURITY IN AFRICA | African Union*. Available at: https://au.int/en/cyberlegislation [Accessed February 16, 2018].

[60] African Union, 2016. Capacity Building for International Cybersecurity Negotiations, Addis Ababa, Ethiopia, 15-16 February 2016. *Capacity Building for International Cybersecurity Negotiations, Addis Ababa, Ethiopia, 15-16 February 2016 | African Union*. Available at: https://au.int/en/newsevents/19716/international-cyber-negotiations [Accessed February 20, 2018].

23. The European Union has the European Commission which proposes and enforces legislation and implements the policies and budgets of the EU[61]. The European Commission has a significant role in the European contributions made toward addressing cyber threats. The EU has started developing strategies to secure their cyberspace since the adoption of the EU Cybersecurity Strategy of 2013 and the Digital Single Market Strategy in 2015. Such strategies discuss the economic potential of using the European cyberspace equally and fairly when it is properly protected and therefore, the fight against cybercrime had been added to the main pillars of the 2015 European Agenda on Security. An example are the goals of the EU cybersecurity strategy of 2013, which aim to increase cyber resilience, reduce cybercrime, develop EU cyber Defence policy, develop industrial and technological resources for cybersecurity, and establish an international cyberspace for the EU. Moreover, in July 2016, the European Parliament adopted the Directive on security of network and information systems (NIS Directive). The NIS Directive is considered an initial step to an EU legislation on cybersecurity[62]. Thus, the aim of such strategies and legislation is to ensure that European nations have equal cybersecurity capabilities and can easily exchange information and cooperate efficiently. In 2004, the EU also launched the European Union Agency for Network and Information Security (ENISA) to ensure information security, network accessibility across the EU, and the prevention of Network and Information Security(NIS) threats[63]. To achieve such goals, ENISA works on collecting and analysing data on security incidents, raising awareness and cooperation between actors in the information security field, and promoting risk assessment and management to deal with emerging threats[64]. The EU has also developed the EU Computer Emergency Response Team (CERT-EU) in 2012. The main aim of this team is to act as a responder to cyber threats or incidents on information security for all the related EU bodies. The EU has also dedicated a significant amount of funding towards measures and initiatives to secure their cyberspace. Between 2007 and 2016, the EU spent an estimated 494 million Euros, and is planning on investing 450 million euros between 2017 to 2020[65]. The EU has been a leader in setting strategies and measures to face cyber threats and thus, it is the perfect example for how a Union can cooperate to deal with the emerging challenges.

ASEAN

24. The Association of Southeast Asian Nations (ASEAN) has been considering the possible threats from the challenges to cybersecurity. The most recent step taken towards this issue was the ASEAN Declaration to Prevent and Combat Cybercrime in November 2017. This was the first declaration to be adopted by the group on the issue of cybercrime directly. It is considered a huge milestone towards securing cyberspace in the region and in increasing cooperation between the group and other organizations such as Interpol. Moreover, the declaration emphasized the importance of law harmonization between nations and on creating a unified approach towards securing

[61] European Union, A., 2018. European Commission - European Union - European Commission. *European Union*. Available at: https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_en [Accessed February 17, 2018].

[62] European Commission, The Directive on security of network and information systems (NIS Directive). *Digital Single Market*. Available at: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive [Accessed February 2, 2018].

[63] European Commission , Cybersecurity . *European Commission* . Available at: http://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf [Accessed February 5, 2018].

[64] European Commission , 2017. Reform of cybersecurity in Europe. *Reform of cybersecurity in Europe - Consilium*. Available at: http://www.consilium.europa.eu/en/policies/cyber-security/ [Accessed February 4, 2018].

[65] European Commission , EU cybersecurity initiatives. *European Commission* . Available at: http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf [Accessed February 2, 2018].

cyberspace[66]. Prior to this declaration, the Association considered the issues of cybercrime as a subtopic to Transnational Crime in 2001 because cybercrime can hardly be linked to one country or place. On the issue of transnational crime, ASEAN adopted the first declaration in 1997 which was signed by all ministers[67]. Following that, they adopted a plan of action to combat transnational crime in 1999[68]. In 2013, a working group was created to tackle the issue of cybercrime and categorize solutions towards it. The issue was divided into five main pillars which were cooperation and information sharing, legal matters and law enforcements, training and capacity building, and regional cooperation between nations[69]. Lastly, ASEAN has been using the ASEAN Regional Forum (ARF) as a platform for constructive dialogue, and political and cooperative consultation[70]. Therefore, the recent efforts of the association clearly show how they are currently considering the threats of cybersecurity as a serious issue.

Possible Solutions

25. *Creation of a Multilateral Framework*
    Information Sharing
    Confidence Building Measures
    Capacity Building
    International Agreed Definitions
    Cooperation between developed and developing nations
    Regional and International Workshops and Summits
    Implementation of new and existing legislations
    Awareness and Propaganda Campaigns
    Further Utilization of the GGE

Current Status

26. The issue of cybersecurity continues to exist and present threats to international security due to a number of factors. Most of those reasons revolve around the idea that certain aspects of the issue are not properly dealt with and Member States decide not to cooperate to address these matters. For example, one of the most significant obstacles is the absence of major international definitions that are crucial to the understanding of the topic. In addition, governments are not cooperating in sharing information about cybersecurity measures and about their cyberspaces due to a lack of trust between them. This creates another challenge and makes it even more difficult for solutions such as confidence building measures to emerge. Another major issue is the absence of cybersecurity systems in half of the world's Member States, which makes their cyber spaces vulnerable to crimes and attacks, and allows criminals to use

[66] ASEAN, 2017. ASEAN DECLARATION TO PREVENT AND COMBAT CYBERCRIME. *ASEAN*. Available at: http://www.asean2017.ph/wp-content/uploads/13-ASEAN-Declaration-to-Combat-Cybercrime.pdf [Accessed January 31, 2018].

[67] ASEAN, ASEAN Declaration on Transnational Crime Manila, 20 December 1997. *ASEAN*. Available at: http://asean.org/?static_post=asean-declaration-on-transnational-crime-manila-20-december-1997 [Accessed February 3, 2018].

[68] ASEAN, ASEAN Plan Of Action To Combat Transnational Crime. *ASEAN*. Available at: http://asean.org/?static_post=asean-plan-of-action-to-combat-transnational-crime [Accessed February 3, 2018].

[69] ASEAN, SEAN WORKING GROUP ON CYBERCRIME. *ASEAN*. Available at: http://asean.org/storage/2012/05/DOC-8-Adopted-TOR-ASEAN-Cybercrime-Working-Group.pdf [Accessed February 4, 2018].

[70] ASEAN, ASEAN Regional Forum (ARF). *ASEAN*. Available at: http://asean.org/asean-political-security-community/asean-regional-forum-arf/ [Accessed February 2, 2018].

such mediums as a method for illicit trafficking and acquiring valuable data and information. To date, there is a huge gap in the security measures for cyberspace around the world – some Member States are more than ready to stop any attack while others do not have an installed defense system. This is a result of the absence of a global manual or procedure which countries can follow or implement. While several regional initiatives on manuals exist, they remain inapplicable to all nations. Lastly, another issue that continues to make it more difficult for Member States to protect their cyber spaces is the transnational nature of cyberattacks, and therefore, cyber-attacks continue to increase day after day.

Key Questions to Consider when Researching and Negotiating:

- How can a more unified approach be initiated to improve cybersecurity globally?
- How can developed nations with active cybersecurity systems help maintain a global cybersecurity system?
- How can weapons be secured from cyber-attacks?
- How can daily users of the internet be protected from cyber threats?
- What kind of definitions should be adopted globally?
- To what extent does cybersecurity threats affect international peace and security?
- How can regional and international manuals for cybercrime incident response be applied effectively?
- How can the Security Council use its mandate to contribute to solving this issue?
- How can the UN and the Security Council prevent the development of cyberwarfare between nations?
- How can the ITU be used to maintain global cybersecurity?
- How can regional blocs be utilized to cooperate against securing their systems against cybercrime?
- What kind of campaigns and propaganda can be launched to create public awareness about cybersecurity challenges?
- How can multilateral agreements be achieved without breaching national sovereignty?
- What kind of platform should be created to increase trust between nations and lead to information sharing?
- How can governments come up with cybersecurity measures without breaching privacy rights of individuals?
- To what extent does the secured usage of ICTs affect the achievement of the Sustainable Development Goals?

Further Research

- Global Security Index
- Cybercrime funded by Member States
- Efforts of the United Nations Office on Drugs and Crime
- Efforts of the United Nations Institute for Disarmament Research
- Efforts of the United Nations Office for Disarmament Affairs
- Council of Europe Octopus Conferences
- Tunis Agenda for the Information Society

- Global Cybersecurity Index
- Internet Governance Forum (IGF)
- Transnational Crime Conventions
- Relevant Group of Governmental Experts (GGE) reports

Useful links

https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf
https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
https://www.itu.int/en/action/cybersecurity/Pages/default.aspx
http://www.tjsl.edu/slomansonb/5.2_TunisAgenda.pdf
https://www.itu.int/net4/wsis/forum/2018/
https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
https://www.un.org/disarmament/topics/informationsecurity/
http://www.unidir.org/est-cyber
https://www.coe.int/en/web/cybercrime/octopus-conference
https://www.coe.int/en/web/cybercrime/capacity-building-programmes
https://news.un.org/en/story/2017/07/560922-half-all-countries-aware-lacking-national-plan-cybersecurity-un-agency-reports
https://www.unsystem.org/content/action-cybersecuritycybercrime
https://www.fbi.gov/investigate/cyber

References and Additional Resources

African Union, DRAFT AFRICAN UNION CONVENTION ON THE ESTABLISHMENT OF A CREDIBLE LEGAL FRAMEWORK FOR CYBERSECURITY IN AFRICA. *DRAFT AFRICAN UNION CONVENTION ON THE ESTABLISHMENT OF A CREDIBLE LEGAL FRAMEWORK FOR CYBERSECURITY IN AFRICA | African Union*. Available at: https://au.int/en/cyberlegislation [Accessed February 16, 2018].

African Union, AFRICAN UNION CONVENTION ON CYBERSECURITY AND PERSONAL DATA PROTECTION. *African Union*. Available at: https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection_1.pdf [Accessed February 19, 2018].

African Union, AFRICAN UNION CONVENTION ON CYBERSECURITY AND PERSONAL DATA PROTECTION. *African Union*. Available at: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf [Accessed February 18, 2018].

African Union, 2016. Capacity Building for International Cybersecurity Negotiations, Addis Ababa, Ethiopia, 15-16 February 2016. *Capacity Building for International Cybersecurity Negotiations, Addis Ababa, Ethiopia, 15-16 February 2016 | African Union*. Available at: https://au.int/en/newsevents/19716/international-cyber-negotiations [Accessed February 20, 2018].

Andrews, E., 2013. Who invented the internet? *History.com*. Available at: http://www.history.com/news/ask-history/who-invented-the-internet [Accessed February 2, 2018].

ASEAN, ASEAN Declaration on Transnational Crime Manila, 20 December 1997. *ASEAN*. Available at: http://asean.org/?static_post=asean-declaration-on-transnational-crime-manila-20-december-1997 [Accessed February 3, 2018].

ASEAN, ASEAN Plan Of Action To Combat Transnational Crime. *ASEAN*. Available at: http://asean.org/?static_post=asean-plan-of-action-to-combat-transnational-crime [Accessed February 3, 2018].

ASEAN, SEAN WORKING GROUP ON CYBERCRIME. *ASEAN*. Available at: http://asean.org/storage/2012/05/DOC-8-Adopted-TOR-ASEAN-Cybercrime-Working-Group.pdf [Accessed February 4, 2018].

ASEAN, ASEAN Regional Forum (ARF). *ASEAN*. Available at: http://asean.org/asean-political-security-community/asean-regional-forum-arf/ [Accessed February 2, 2018].

ASEAN, 2017. ASEAN DECLARATION TO PREVENT AND COMBAT CYBERCRIME. *ASEAN*. Available at: http://www.asean2017.ph/wp-content/uploads/13-ASEAN-Declaration-to-Combat-Cybercrime.pdf [Accessed January 31, 2018].

Ashford, W. ed., 2018. Nuclear weapons' cyber attack risk relatively high, says report. *ComputerWeekly*. Available at: http://www.computerweekly.com/news/450432994/Nuclear-weapons-cyber-attack-risk-relatively-high-says-report [Accessed February 14, 2018].

Clickatell, Cybercrime and its effect on businesses. *Clickatell*. Available at: https://www.clickatell.com/articles/information-security/cybercrime-effect-businesses/ [Accessed February 5, 2018].

Commonwealth, 2018. Commonwealth Cybercrime Initiative. *Commonwealth Cybercrime Initiative | The Commonwealth*. Available at: http://thecommonwealth.org/commonwealth-cybercrime-initiative [Accessed February 4, 2018].

Council, Y.E., 2017. The True Cost Of Cybercrime For Businesses. *Forbes*. Available at: https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#8d5109349476 [Accessed February 4, 2018].

Council of Europe, Reports. *Cybercrime*. Available at: https://www.coe.int/en/web/cybercrime/all-reports [Accessed January 19, 2018].

Council of Europe, Convention on Cybercrime. *Council of Europe*. Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [Accessed February 14, 2018].

Council Of Europe, 2003. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. *Council Of Europe*. Available at: http://www.notohatespeech.com/wp-content/uploads/2016/08/AP-Cybercrime.pdf [Accessed January 21, 2018].

Council of Europe, 2018. Chart of signatures and ratifications of Treaty 185. *Council of Europe*. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures [Accessed February 22, 2018].

Department of Homeland Security, 2017. Office of Cybersecurity and Communications. *Department of Homeland Security*. Available at: https://www.dhs.gov/office-cybersecurity-and-communications [Accessed February 2, 2018].

Dictionary.com, cyberspace. *Dictionary.com*. Available at: http://www.dictionary.com/browse/cyberspace?s=t [Accessed February 1, 2018].

Dictionary.com, cybersecurity. *Dictionary.com*. Available at: http://www.dictionary.com/browse/cybersecurity?s=t [Accessed February 1, 2018].

Dictionary.com, cybercrime . *Dictionary.com*. Available at: http://www.dictionary.com/browse/cybercrime?s=t [Accessed February 13, 2018].

Eggers, W.D., 2016. Government's cyber challenge: Protecting sensitive data for the public good. *Deloitte Insights*. Available at: https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/protecting-sensitive-data-government-cybersecurity.html [Accessed January 30, 2018].

European Commission, The Directive on security of network and information systems (NIS Directive). *Digital Single Market*. Available at: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive [Accessed February 2, 2018].

European Commission , EU cybersecurity initiatives. *European Commission* . Available at: http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf [Accessed February 2, 2018].

European Commission , Cybersecurity . *European Commission* . Available at: http://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf [Accessed February 5, 2018].

European Commission , 2017. Reform of cybersecurity in Europe. *Reform of cybersecurity in Europe - Consilium*. Available at: http://www.consilium.europa.eu/en/policies/cyber-security/ [Accessed February 4, 2018].

European Union, A., 2018. European Commission - European Union - European Commission. *European Union*. Available at: https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_en [Accessed February 17, 2018].

First, FIRST History. *FIRST - Forum of Incident Response and Security Teams*. Available at: https://www.first.org/about/history [Accessed February 15, 2018].

First, FIRST Vision and Mission Statement. *FIRST - Forum of Incident Response and Security Teams*. Available at: https://www.first.org/about/mission [Accessed February 15, 2018].

Global Forum on Cyber Expertise, 2016. The Budapest Convention on Cybercrime: a framework for capacity building. *Global Forum on Cyber Expertise*. Available at: https://www.thegfce.com/news/news/2016/12/07/budapest-convention-on-cybercrime [Accessed February 22, 2018].

GOV.UK, Cyber and Government Security Directorate. *Cyber and Government Security Directorate - GOV.UK*. Available at: https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance [Accessed February 3, 2018].

InfoSec Institute, 2015. 2013 - The Impact of Cybercrime. *InfoSec Resources*. Available at: http://resources.infosecinstitute.com/2013-impact-cybercrime/#gref [Accessed February 12, 2018].

Interpol, Overview. *Overview / About INTERPOL / Internet / Home - INTERPOL*. Available at: https://www.interpol.int/About-INTERPOL/Overview [Accessed February 23, 2018].

Interpol, Cybercrime. *Cybercrime / Cybercrime / Crime areas / Internet / Home - INTERPOL*. Available at: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime [Accessed February 23, 2018].

Interpol, The INTERPOL Global Complex for Innovation. *The INTERPOL Global Complex for Innovation / About INTERPOL / Internet / Home - INTERPOL*. Available at:

https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation [Accessed February 23, 2018].

ITU, 2018. Goal 5. Gender. *ITU*. Available at: https://www.itu.int/en/sustainable-world/Pages/goal5.aspx [Accessed February 11, 2018].

ITU, 2018. Goal 9. Infrastructure, Industrialization, Innovation. *ITU*. Available at: https://www.itu.int/en/sustainable-world/Pages/goal9.aspx [Accessed February 11, 2018].

ITU, 2018. Goal 11. Cities. *ITU*. Available at: https://www.itu.int/en/sustainable-world/Pages/goal11.aspx [Accessed February 11, 2018].

ITU, 2018. Goal 17. Implementation. *ITU*. Available at: https://www.itu.int/en/sustainable-world/Pages/goal17.aspx [Accessed February 11, 2018].

Morgan, S., 2017. Is cybercrime the greatest threat to every company in the world? *Cybersecurity Business Report*. Available at: Is cybercrime the greatest threat to every company in the world? [Accessed January 31, 2018].

Nations, United Nations Official Document. *United Nations*. Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A%2FRES%2F53%2F70 [Accessed February 1, 2018].

NUS, 2008. History of ICT. *Wiki.nus*. Available at: https://wiki.nus.edu.sg/display/cs1105groupreports/History of ICT [Accessed February 23, 2018].

Public Knowledge, 2018. Cybersecurity and Human Rights. *Public Knowledge*. Available at: https://www.publicknowledge.org/cybersecurity-and-human-rights [Accessed February 10, 2018].

Security Council, 2007. Cooperation with International, Regional and Subregional Organizations | UN Counter-Terrorism Committee. *United Nations*. Available at: http://www.un.org/en/sc/ctc/cooperation.html [Accessed February 15, 2018].

Statista, 2018. Number of internet users worldwide 2005-2017. *Statista*. Available at: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/ [Accessed February 3, 2018].

Statista, 2018. Number of mobile phone users worldwide 2013-2019. *Statista*. Available at: https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/ [Accessed February 3, 2018].

Terebey, S., 2017. African Union Cybersecurity Profile: Seeking a Common Continental Policy. *The Henry M. Jackson School of International Studies*. Available at: https://jsis.washington.edu/news/african-union-cybersecurity-profile-seeking-common-continental-policy/ [Accessed February 7, 2018].

United Nations, Developments in the field of information and telecommunications in the context of international security – UNODA. *United Nations*. Available at: https://www.un.org/disarmament/topics/informationsecurity/ [Accessed February 11, 2018].

United Nations, Resolution Adopted by the General Assembly. *United Nations*. Available at: https://undocs.org/A/RES/53/70 [Accessed January 31, 2018].

United Nations, Resolution adopted by the General Assembly. *United Nations*. Available at: https://undocs.org/A/RES/58/32 [Accessed February 11, 2018].

United Nations, Resolution Adopted by the General Assembly. *United Nations*. Available at: http://undocs.org/A/RES/68/167 [Accessed February 14, 2018].

United Nations, Resolution Adopted by the General Assembly. *United Nations*. Available at: https://undocs.org/A/RES/69/28 [Accessed February 15, 2018].

United Nations, ICTs for a Sustainable World #ICT4SDG. *ICTs for a Sustainable World #ICT4SDG*. Available at: https://www.itu.int/en/sustainable-world/Pages/default.aspx [Accessed February 2, 2018].

United Nations, Overview. *ITU*. Available at: https://www.itu.int/en/about/Pages/overview.aspx [Accessed February 21, 2018].

United Nations, Global Cybersecurity Agenda (GCA). *Global Cybersecurity Agenda (GCA)*. Available at: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx [Accessed February 12, 2018].

United Nations, World Summit on the Information Society (WSIS) .:. Sustainable Development Knowledge Platform. *United Nations*. Available at: https://sustainabledevelopment.un.org/index.php?page=view&type=30022&nr=102&menu=3170 [Accessed February 17, 2018].

United Nations, 2018. Security Council, SC, UNSC, security, peace, sanctions, veto, resolution, president, united nations, UN, peacekeeping, peacebuilding, conflict resolution, prevention. *United Nations*. Available at: http://www.un.org/en/sc/about/ [Accessed February 14, 2018].

United Nations, 2018. Security council, SC, UNSC, security, peace, sanctions, veto, resolution, president, united nations, UN, peacekeeping, peacebuilding, conflict resolution, prevention. *United Nations*. Available at: http://www.un.org/en/sc/about/functions.shtml [Accessed February 23, 2018].

United Nations , 2017. Countering Illicit Arms Trafficking and its Links to Terrorism and Other Serious Crime UNODC's Global Firearms Programme. *United Nations* . Available at: https://www.un.org/sc/ctc/wp-content/uploads/2017/05/Simonetta-UNODC-at-CTED_May2017v2.pdf [Accessed January 31, 2018].

USAID, Cyber Crime: Its Impact on Government, Society and the Prosecutor. *USAID*. Available at: http://pdf.usaid.gov/pdf_docs/Pnada641.pdf [Accessed January 31, 2018].

USAID, Cyber Crime: Its Impact on Government, Society and the Prosecutor. *USAID*. Available at: http://pdf.usaid.gov/pdf_docs/Pnada641.pdf [Accessed January 31, 2018].

Veritas Global, 2018. News Release. *Veritas Global Databerg Report Finds 85% of Stored Data Is Either Dark, or Redundant, Obsolete, or Trivial (ROT)*. Available at: https://www.veritas.com/news-releases/2016-03-15-veritas-global-databerg-report-finds-85-percent-of-stored-data [Accessed February 1, 2018].