Committee: Disarmament and International Security Committee

Topic: Methods of enhancing cyber security via technological advancements

Student officer: Adriano Souras

Position: Deputy Chair

PERSONAL INTRODUCTION

Dear Delegates,

My name is Adrianos Souras, and I am honored and excited to be the Co-Chair in the Disarmament and International Security Committee in the upcoming CS MUN conference. My experience with MUN has been a paradigm-shifting one for sure. This is going to be my third time chairing and the 12th MUN conference I attend as a whole.

MUN for me other than being the perfect time to meet like-minded people is also an event that allows me to reflect on today's events. The question of enhancing methods of cybersecurity via technological advancements is a truly dire issue and reflects stability and reliance we have on said technology hence making this issue a matter of urgency for the Disarmament and International Security Committee.

Apart from this study guide, which will serve as a pretext to your investigation, I highly advise you to extend your knowledge and that you research your delegation’s policy thoroughly. In the case where any questions may arise, feel free to contact me at any time through my email (adriano.souras@gmail.com). I wish you the best of luck in your future endeavors and preparation regarding this issue and I am very happy to meet you all!

Sincerely,

Adrianos

INTRODUCTION

As technology advances, new ways have to be found in order to enhance the security of electronic data. It is significant to tackle this issue both on a personal level as well as in the interest of national security. Following important events such as the controversy between Facebook and Cambridge Analytica and the implementation of GDPR (General Data Protection Regulation), much progress has been done to resolve this issue and strengthen cyber security. Cyber security is essential as it affects everyone nowadays. It is extremely easy for cyber criminals to gain access to our data, therefore enhancing cyber security currently, is of great need. Any sort of data could be stolen by hackers, from social media accounts, to bank accounts, with just a few clicks on a computer keyboard. What's more, is that this happens everyday. Cyber criminals invade one's privacy everyday, whether those people shop online, bank, or receive money online. The fact that most people are so unaware of this danger makes them vulnerable which makes cyber criminals' job much easier. As delegates, it is your responsibility to come up with further solutions in order to strengthen cyber security for the protection of countries from international criminals and hackers, as well as ordinary people from organizations seeking to exploit their personal data.

DEFINITIONS OF KEY TERMS

Cyber

Relating to, or involving computers or computer networks (such as the Internet)[1]

Cyber-Crime

Cybercrime is any criminal activity that involves a computer, networked device or a network.[2]

[1] "Cyber." *Merriam-Webster*, Merriam-Webster, https://www.merriam-webster.com/dictionary/cyber.
[2] "What Is Cybercrime? - Definition from WhatIs.com." *SearchSecurity*, https://searchsecurity.techtarget.com/definition/cybercrime.

Cyber-security

Cyber-security or information technology security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation[3]

Cyber-warfare

Cyberwarfare is a broad term describing the use of technological force within cyberspace. 'Cyberwarfare' does not imply scale, protraction or violence which are typically associated with the term 'war'. [4]

Blockchain

A system in which a record of transactions made in bitcoin or another cryptocurrency are maintained across several computers that are linked in a peer-to-peer network.[5]

Cloud Technology

The term is generally used to describe data centers available to many users over the Internet.[6]

IoT Security

IoT security is the technology area concerned with safeguarding connected devices and networks in the internet of things. IoT involves adding internet connectivity to a system of interrelated computing devices, mechanical and digital machines, objects, animals and/or people.[7]

Deep Learning

---

[3] ''What Is Cyber Security? Definition of Cyber Security, Cyber Security Meaning." *The Economic Times*, https://economictimes.indiatimes.com/definition/cyber-security.
[4]"Cyberwarfare." *Wikipedia*, Wikimedia Foundation, 12 Sept. 2019, https://en.wikipedia.org/wiki/Cyberwarfare.
[5] Gupta, Hargobind. "What Blockchain Is Not?" *Medium*, Medium, 26 Mar. 2019, https://medium.com/@hargobindgupta/what-blockchain-is-not-e4afa0d603f2.
[6] "Cloud Computing." *Wikipedia*, Wikimedia Foundation, 12 Sept. 2019, https://en.wikipedia.org/wiki/Cloud_computing.
[7] "What Is IoT Security (Internet of Things Security)? - Definition from WhatIs.com." *IoT Agenda*, https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security.

Deep learning is a subset of machine learning where artificial neural networks, algorithms inspired by the human brain, learn from large amounts of data.[8]

Espionage and national security breaches

Cyber espionage is the act or practice of obtaining secrets (sensitive, proprietary or classified information) from individuals, competitors, rivals, groups, governments and enemies for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers. Classified information that is not handled securely can be intercepted and even modified, making espionage possible from the other side of the world

[8] Marr, Bernard. "What Is Deep Learning AI? A Simple Guide With 8 Practical Examples." *Forbes*, Forbes Magazine, 12 Dec. 2018, https://www.forbes.com/sites/bernardmarr/2018/10/01/what-is-deep-learning-ai-a-simple-guide-with-8-practical-examples/.

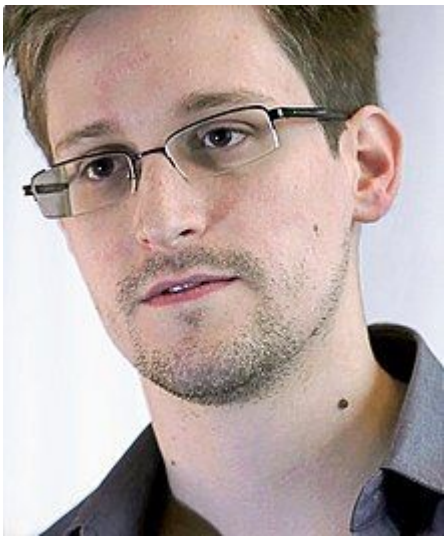
TIMELINE

1976	Data encryption standard is approved for the first time
1984	Robert Schifreen and Steve Gold, british hackers, are arrested for hacking into Price Phillip's personal email. For more information click here.
1985	The first ever virus is created in Pakistan called the "Brain". It is used for stealth techniques. For more information click here.
1988	The words "hacker," and "cracker," are first used in the media
1988	Robert Morris releases the Internet Worm and spreads to 10% of all computers on the internet. For more information click here.
1990	The computer misuse act is ratified in the UK. For a complete explanation click here.
1994	Kaos virus is launched and attacks a newsgroup for more information visit:
1995	Hackers manage to change the interface of the US Justice Department, the CIA, and the US Air Force. If you wish to find out more click here.

1998	First Denial of Service attack on a large scale takes place, targeting universities across the US as well as the US navy. MS Windows NT and Windows 95 software users were vulnerable. To find out more about this specific event or about Denial of Service attacks go here.
1998	Carl-Fredrick Neikter releases the Netbus Trojan tool, which allows hackers to obtain remote access to infected machines. For a further explanation click here.
1998	AOL Trojans are programmed. They were designed for stealing information from America Online users. For a detailed explanation click here.
1999	Distributed Network sniffers are used to capture usernames and passwords. Linux operating system hosts are compromised
2000	The NIPC issues a security advisory regarding increased illegal hacker activity against the US e-commerce and Internet-hosted systems. For a more detailed report click here.
2003	US/NATO introduces five pillars which then becomes the gold standard for the rest of the nations in the UN. For more info click here.

BACKGROUND INFORMATION

Past Cyber Attacks



Cyber-crime is a multifaceted and complex topic. For one, cyber-attacks can be used as a method of activism, such as in the case of Wikileaks. Wikileaks is an organisation that serves as a platform for anonymous whistleblowers to publish news leaks and classified media.[9] The most noteworthy instance being that of Edward Snowden. Edward Snowden is from Elizabeth City, North Carolina. In 2003, after his brief attendance at Maryland Community College, he joined the United States of America Army and began training to become part of the special forces. However, he was discharged after breaking both of his legs in an accident. He then joined the Central Intelligence Agency (CIA) and climbed the ranks due to his abilities. In 2009 he joined the National Security Agency (NSA)[10]. This is where Mr. Snowden reportedly saw the abuse. Soon after, in collaboration with the Guardian in June 2013 the article, "NSA collecting phone records of millions of Verizon customers daily" which marked the beginning of a series of exposé articles based on leaked top-secret documents showing that the National Security Agency was spying on American citizens.

The very first article revealed that Verizon (a mobile data provider in the United States of America) had given the NSA a backdoor to spy on their customers. Later on, it was proven that Verizon was not the only company doing so but rather most were.[11] The second article was regarding an NSA project called PRISM. In the beginning, PRISM was described as a program that gave the NSA direct access to tech companies like Google, Facebook,

---

[9]"Major Civil Liberties, Media Freedom, and Human Rights Groups Speak out against the Arrest of Julian Assange." *Common Ground*, 16 May 2019, https://commonground.ca/groups-against-julian-assnage-arrest/.
[10] "Profile: Edward Snowden." *BBC News*, BBC, 16 Dec. 2013, https://www.bbc.com/news/world-us-canada-22837100.
[11] Greenwald, Glenn. "NSA Collecting Phone Records of Millions of Verizon Customers Daily." *The Guardian*, Guardian News and Media, 6 June 2013, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Microsoft and Apple. However, in reality PRISM was proven to be far less extreme, in fact, it could merely request the tech companies for data regarding specific things[12]. In addition, another program called "XKeyscore" was leaked. This program allows the NSA to access all the internet activity of specific people they want to spy on. [13]

This event as a whole on a historic level is very important. It marks the first time where there is viable evidence to show how the government spies on its citizens. It is also important to note that in this instance, it is actually very disputed whether it counts as cyber-crime or not. Nonetheless, we can see how hacking can be used in a Robin Hood-like way, where even though numerous laws are broken, the ends justify the means.

Another example of cyber-crime being used for activism is the Aramco Hack. In this case 35,000 computers from Saudi Aramanco were breached.[14] The virus was called Shamoon and projected an image of an American flag on fire on the screens of the computers of all employees. [15] The Aramco incident shows a paradigm shift in hacking, from a fashionable trend to a criminal mechanism.

The next instance was the mosquito program that goes even deeper into the concept of hacking as a spy and company approach. The Mosquito program engaged two people, Brown and Scott, who had developed a company called Ephemeral Security that was employed to hack companies and banks, stealing their own data, and then pointing out the system's faults to avoid other hackers. What followed next was a program called mosquito developed by both of them and intended to collect data during penetration trials. But this was more than just a testing instrument, as the concept of the two men was also a revolutionary model for spying. Such mosquito-like malware proved helpful for a few tricks.

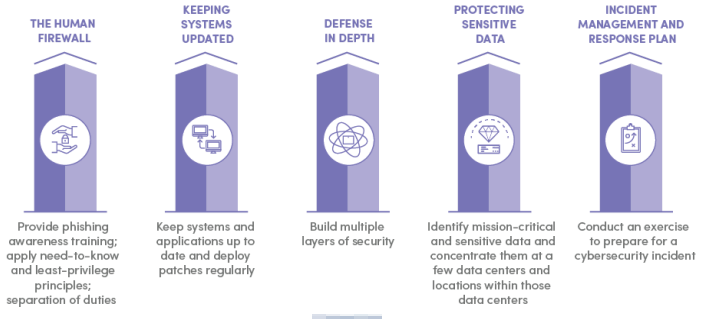
---

[12] Franceschi-Bicchierai, Lorenzo. "Edward Snowden: The 10 Most Important Revelations From His Leaks." *Mashable*, 5 June 2014, https://mashable.com/2014/06/05/edward-snowden-revelations/?europe=true.
[13] "XKeyScore." *Courage Snowden*, https://freesnowden.is/2013/07/31/xkeyscore-training-materials/.
[14] time, And for the first. "The inside Story of the Biggest Hack in History." *CNNMoney*, Cable News Network, https://money.cnn.com/2015/08/05/technology/aramco-hack/.
[15]"BullGuard Blog." *BullGuard*, https://www.bullguard.com/blog/2016/07/cyber-armageddon.

One could hack into one's microphone and record the environment of the machine or examine architectural plans and design schemes, analyzing the internal functioning of industrial facilities. [16]

What one should extract from the event is that not only was hacking reincarnated into a business plan in this case, but, in essence, operating as an integral part of the system. Indeed, in a market-oriented fight, Cyber Warfare stands as an antagonistic "weapon."

Causes of Cyber Attacks



As we and governments have developed a huge reliance on computer systems to carry out daily businesses as well as developed an inherent trust in these systems it is safe to say that we have placed incredibly important and valuable information on them. Hence, with that said, when there is a breach the consequences may be detrimental. It is this flood of information that puts a target on our backs. [17]

With the invention of the modern day web browser and email in the 90s also came the invention of a new platform and new tools for cybercriminals to exploit. From having to initiate a physical transaction, such as giving them a faulty harddrive, hackers could transmit malware over the internet to affect millions. In the dawn of the 21st century and the introduction of social media, there was a rise in identity theft. Social Media platforms would have personal data of all their users on databases with weak firewalls. Hackers would get remote access to these and sell private information to the highest bidder. The impact was enormous; through obtaining this personal information people easily managed to open up bank accounts and commit financial fraud on a previously unprecedented level.

Furthermore, as suggested above cybercrime is a very in-depth topic. As a result, the causes vary throughout every single attack. However, many researchers have deduced that the main reason for cyber breaches is to show that they can. Many hackers find hacking into

---

[16] "Hacker – What Is Hacking and How to Protect Yourself." *Malwarebytes*, https://www.malwarebytes.com/hacker/.
[17] "The Evolution of Cybercrime." *Packt Hub*, 3 Apr. 2018, https://hub.packtpub.com/the-evolution-cybercrime/.

different corporations as accolades and challenges, similar to an obstacle course. On the one hand, this may seem as somewhat innocent however there is a slight proportion who have malicious intent. It could be suggested that this may be because of financial problems and wealth inequality; young great minds that are forced to commit crimes in pursuit of monetary gains. Finally, another reason for cyber attacks is cyber warfare; nations attacking each others' databases to acquire information about matters of national security.

MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

United States of America

The USA's mission statement in regards to cybersecurity is, "United States Cyber Command plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defence of specified Department of Defence information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[18] This mission statement shows the USA's full support for cyber security.

Russia

By submitting a resolution to the First Committee in 1998 Russia was the first country to address cybersecurity in the UN formally. In 2010, Russian delegates considered the issue of cyber-attacks the most serious of challenges in the 21st century, and followed up in 2011 by publishing a convention on International Information Security.

In fact, Russia in 2008 was accused of hacking numerous eastern European countries. Russia is once again under the spotlight with the recent events of Edward Snowden and WikiLeaks.

[18] staff, Science X. "US Cyber Command Logo Contains Coded Message." *Phys.org*, Phys.org, 8 July 2010, https://phys.org/news/2010-07-cyber-logo-coded-message.html.

France

France's mission statement is as follows: "operational cooperation needs to be stepped up between EU Member States. The aim is to establish pan-European tools to share technical information on threats, supporting preparation and rapid response in the event of cyber attacks. The creation in 2017 of the EU Cyber Diplomacy Toolbox (CDT) to combat cyber attacks is a full-fledged aspect of this cooperation."[19] We can see that France even though in the center of many allegations has taken a position to further develop infrastructure to protect member-states.

China

China has been accused of cyber warfare on countries including Australia, India, Canada and the USA. Most recently, China has suspended the Cybersecurity Cooperation with the USA after being charged with cybercrime.[20] In addition, China was actually one of the first countries along with Russia to bring up the issue in the first place. Furthermore China has implemented many laws as well to prevent this from happening. Such as but not limited to: Article 285 which directly addresses invading a computer system in the area of State Affairs would be punishable by being fined and the people that are viable punished accordingly; Article 286 which states that "crime of sabotaging a computer information system would be penalised by five years in federal prison." [21]

Germany

[19] Ministère de l'Europe et des Affaires étrangères. "France Diplomatie - MEAE." *France Diplomatie :: Ministry for Europe and Foreign Affairs*, https://www.diplomatie.gouv.fr/en/.

[20] Selyukh, Alina. "China Cyber Crime Cooperation Stalls after U.S. Hacking Charges." *Reuters*, Thomson Reuters, 26 June 2014, https://www.reuters.com/article/us-usa-cybersecurity-china-idUSKBN0F12OJ20140626.

[21] "Cybersecurity 2019: Laws and Regulations: China: ICLG." *International Comparative Legal Guides International Business Reports*, Global Legal Group, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/china.

Germany's mission statement shows full compliance with previous endeavors: "the Federal Government aims at making a substantial contribution to a secure cyberspace, thus maintaining and promoting economic and social prosperity in Germany. Cyber security in Germany must be ensured at a level commensurate with the importance and protection required by interlinked information infrastructures, without hampering the opportunities and the utilization of the cyberspace. In this context the level of cyber security reached is the sum of all national and international measures taken to protect the availability of information and communications technology and the integrity, authenticity and confidentiality of data in cyberspace."

UK

UK members of parliament have synthesised the following, "Cyber is a Tier 1 threat to the UK's economic and national security. The policies, institutions, and initiatives developed under the previous strategy have helped to establish the UK as a leading global player in cybersecurity. However, the scale and dynamic nature of cyber threats, and the increasing dependency of our economy and society on digital products and services mean that our current approach to cyber security needs to be further strengthened. Therefore, the Government is today publishing the new five year National Cyber Security Strategy, which defines our vision and ambition for achieving a UK that is secure and resilient to cyber threats; prosperous and confident in the digital world."[22]

Global Cybersecurity Agenda (GCA)

The International Telecommunications Union (ITU) launched the Global Cybersecurity Agenda (GCA) in 2007, which serves as a practical framework for collaborating on cyber security for all 193 Member States.

[22] author, EPSRC. "Grants on the Web." *EPSRC Centre for Doctoral Training in Cyber Security for the Everyday*, Engineering and Physical Sciences Research Council, Polaris House, North Star Avenue, Swindon, SN2 1ET, https://gow.epsrc.ukri.org/NGBOViewGrant.aspx?GrantRef=EP/S021817/1.

In addition, the GCA comprises of five pillars. First, "legal measures" focus on pursuing illegitimate cyber operations with an internationally coherent parliamentary approach. Second, "technical and procedural measures" address the safety requirements of ICT apps and systems and best risk management practices.Third, "organisational structures" discuss domestic policies and institutional arrangements that enable efficient cyberattack prevention, reaction, and crisis management. Fourth, "capacity building" promotes sharing among all stakeholders of knowledge and technology. And the last pillar, "global cooperation," encourages international community dialog and coordinated action to address cyber threats.

United Nations Office on Drugs and Crime

The United Nations Office on Drugs and Crime is a United Nations office that was established in 1997 as the Office for Drug Control and Crime Prevention by combining the United Nations International Drug Control Program and the Crime Prevention and Criminal Justice Division of the United Nations Office at Vienna.

The Global Forum on Cyber Expertise

The Global Forum on Cyber Expertise (GFCE) is a global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building. The aim is to identify successful policies, practices and ideas and multiply these on a global level. Together with partners from NGOs, the tech community and academia GFCE members develop practical initiatives to build cyber capacity.

UN INVOLVEMENT: RELEVANT RESOLUTIONS AND TREATIES

70/237[23]

Extended the initial resolution by setting up a group of governmental specialists.

58/32[24]

Addressed the respect for human rights and basic liberties.

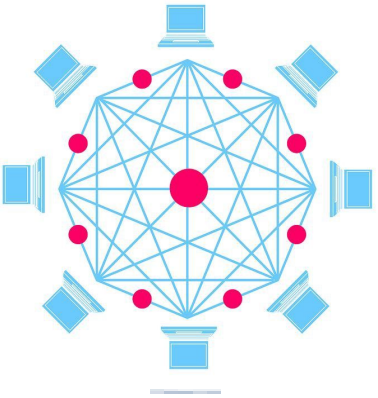
64/211[25]

This resolution raised further awareness of the magnitude of cyber crime to Member States.

POSSIBLE SOLUTIONS

The best way to deal with viable battle cybercrime requires worldwide cooperation, furthermore a universal body that can intervene in question and dispatch assets to share data about cybercrime patterns. A focal revealing and data sharing channel between the private and open divisions are required. The best case of this sort of data sharing up to this point is FIRST (Forum of Incident Response and Security Teams), around 1990. With regards to law requirement, shifting wards and laws confuse the arraignment of cybercriminals. However, numerous assaults are dealt with outside this discussion and specially appointed wrongdoing.

Furthermore, another possible solution may be to move everything on blockchain, and increase anonymity and



[23] *A/RES/70/237 - E - A/RES/70/237*, https://undocs.org/A/RES/70/237.
[24] *A/RES/58/32 - E - A/RES/58/32*, https://undocs.org/A/RES/58/32.
[25] *A/RES/64/211 - E - A/RES/64/211*, https://undocs.org/A/RES/64/211.

security, as all information will be scattered on thousands of servers making hacking virtually impossible. However, this solution taking into account the current infrastructure is not necessarily realistic.

On a more pragmatic level another solution is through education. In numerous countries in the European Union there has been an emergence of tech classes, through compelling legislation this can be brought to a global level where kids learn how to protect themselves online and learn about the drastic effects of cyber-crime as well as the repercussions of doing so.

A stated above a huge cause of cyber crime is our dependance on the web and the amount of information we place on our digital footprint. As delegates I suggest you formulate ideas about setting up bureaucratic means to make putting vital information not necessary and hence to accessible to hackers.

BIBLIOGRAPHY

Bell, Steve. “Cyber Armageddon.” *BullGuard Blog*, BullGuard, 7 July 2016, www.bullguard.com/blog/2016/07/cyber-armageddon.

Editorial Staff, Packt. “The Evolution of Cybercrime.” *A History of Cybercrime*, Packt Hub, 3 Apr. 2018, hub.packtpub.com/the-evolution-cybercrime/.

EPSRC. “Grants on the Web.” *EPSRC Centre for Doctoral Training in Cyber Security for the Everyday*, Engineering and Physical Sciences Research Council, Polaris House, North Star Avenue, Swindon, SN2 1ET, 2011, gow.epsrc.ukri.org/NGBOViewGrant.aspx?GrantRef=EP%2FS021817%2F1.

Franceschi-Bicchierai, Lorenzo. “Edward Snowden: The 10 Most Important Revelations From His Leaks.” *Mashable*, Mashable, 5 June 2014, mashable.com/2014/06/05/edward-snowden-revelations/?europe=true.

German Ministry of Defense. *Cyber Security Strategy for Germany*. Enisa.europa, 2013.

Greenwald, Glenn. “NSA Collecting Phone Records of Millions of Verizon Customers Daily.” *The Guardian*, Guardian News and Media, 6 June 2013, www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Gupta , Hargobind. “What Blockchain Is Not? - Hargobind Gupta.” *What Blockchain Is Not?*, Medium, 26 Mar. 2019, medium.com/@hargobindgupta/what-blockchain-is-not-e4afa0d603f2.

Gupta , Sergi. “Definition of Cyber Security: What Is Cyber Security ? Cyber Security Meaning.” *The Economic Times*, 2018, economictimes.indiatimes.com/definition/cyber-security.

“Hacker – What Is Hacking and How to Protect Yourself.” *What Is Hacking*, Malwarebytes, www.malwarebytes.com/hacker/.

“Major Civil Liberties, Media Freedom, and Human Rights Groups Speak out against the Arrest of Julian Assange.” *Common Ground*, Surveillance Capitalism , 8 May 2019, commonground.ca/groups-against-julian-assnage-arrest/.

Marr, Bernard. “What Is Deep Learning AI? A Simple Guide With 8 Practical Examples.” *Forbes*, Forbes Magazine, 12 Dec. 2018, www.forbes.com/sites/bernardmarr/2018/10/01/what-is-deep-learning-ai-a-simple-guide-with-8-practical-examples/#6e5892aa8d4b.

Merriam. “Cyber.” *Merriam-Webster*, Merriam-Webster, 2013, www.merriam-webster.com/dictionary/cyber.

Ministère de l'Europe et des Affaires étrangères. “France Diplomatie - MEAE.” *France Diplomatie :: Ministry for Europe and Foreign Affairs*, 2015, www.diplomatie.gouv.fr/en/.

Ning, Susan, and Han Wu. “Cybersecurity 2019: Laws and Regulations: China: ICLG.” *International Comparative Legal Guides International Business Reports*, Global Legal Group, 16 Oct. 2018, iclg.com/practice-areas/cybersecurity-laws-and-regulations/china.

Pagliery, Jose. “The inside Story of the Biggest Hack in History.” *CNNMoney*, Cable News Network, 5 Aug. 2015, 2:31 PM ET, money.cnn.com/2015/08/05/technology/aramco-hack/.

Poitras, Laura, et al. "'A' For Angela: GCHQ and NSA Targeted Private German Companies and Merkel - SPIEGEL ONLINE - International." *International*, SPIEGEL ONLINE, 29 Mar. 2014, www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html.

"Profile: Edward Snowden." *BBC News*, BBC, 16 Dec. 2013, www.bbc.com/news/world-us-canada-22837100.

Rouse, Margaret, et al., "What Is Cybercrime? - Definition from WhatIs.com." *SearchSecurity*, 2014, searchsecurity.techtarget.com/definition/cybercrime.

Rouse, Margaret, et al., "What Is IoT Security (Internet of Things Security)? - Definition from WhatIs.com." *IoT Security (Internet of Things Security)*, IoT Agenda , Oct. 2018, internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security.

Selyukh, Alina. "China CyberCrime Cooperation Stalls after U.S. Hacking Charges." *Reuters*, Thomson Reuters, 26 June 2014, www.reuters.com/article/us-usa-cybersecurity-china-idUSKBN0F12OJ20140626.

staff, Science X. "US Cyber Command Logo Contains Coded Message." *Phys.org*, Phys.org, 8 July 2010, phys.org/news/2010-07-cyber-logo-coded-message.html.

"Timeline of Major Events in Internet Security ." *Symantec Security Response*, Symantec, 2006.

Trustees of Courage. "In Support of Edward Snowden." *XKeyScore*, Free Snowden, 2013, freesnowden.is/2013/07/31/xkeyscore-training-materials/.

Wang. “Cloud Computing.” *Wikipedia*, Wikimedia Foundation, 17 July 2019, en.wikipedia.org/wiki/Cloud_computing.

Warren, Peter. “Cyberwarfare.” *Wikipedia*, Wikimedia Foundation, 15 July 2019, en.wikipedia.org/wiki/Cyberwarfare.