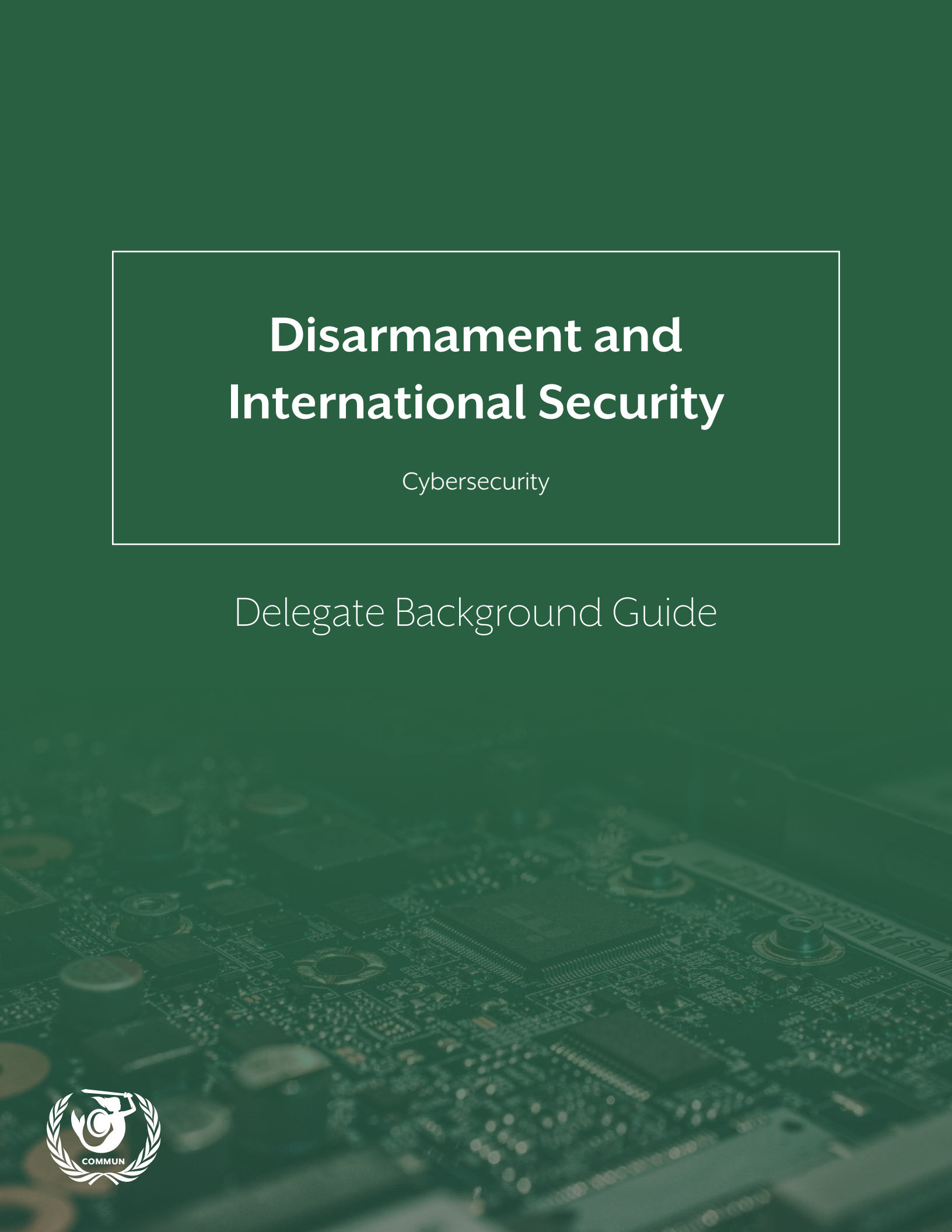
Disarmament and International Security

Cybersecurity

Delegate Background Guide



A Letter from Your Chairs...

Dear Delegates,

I hope this background guide finds you well. I'm Romen Der Manuelian, Chair of the Disarmament and International Security Committee (DISEC) at COMMUN. I'm a sophomore, and this is my first time chairing a UNAGB conference. I've been engaged in Model UN for 5 years now. I and my Co-Chair William Du cordially welcome you to discuss the tasks of the DISEC mentioned below. The topic of concern in our session is cybersecurity and the rules and penalties around it. Cybersecurity contains many of the most challenging aspects of national security, privacy, safety, and technological and economic growth. Cyberspace has become the future of defense, economics, and business, and is most used by common people for communication. Delegates, your goal is to reach a consensus within this committee, despite conflicting beliefs between your respective nations that could never go in the same working paper and resolution. We not only expect there to be conflicts over your resolutions because of the debate around this from many different nation's perspectives but encourage it as well. If you have any questions, I invite you to email me or my Co-Chair, at rdermanuelian@commschool.org or wdu@commschool.org so there is as little confusion as possible on the topic on the day of the conference.

All the best, and good luck.

Romen Der Manuelian
Chair
rdermanuelian@commschool.org

William Du
Co-Chair
wdu@commschool.org

Table of Contents

Introduction

> "Why did I decide to write cyber thrillers? Because we've gone from the Cold War to the Code War."
>
> — Thomas Waite

DISEC Committee Purpose and Function

"[DISEC] deals with disarmament, global challenges, and threats to peace that affect the international community and seeks out solutions to the challenges in the international security regime. It considers all disarmament and international security matters within the scope of the Charter or relating to the powers and functions of any other organ of the United Nations; the general principles of cooperation in the maintenance of international peace and security, as well as principles governing disarmament and the regulation of armaments; promotion of cooperative arrangements and measures aimed at strengthening stability through lower levels of armaments. The Committee works in close cooperation with the United Nations Disarmament Commission and the Geneva-based Conference on Disarmament. It is the only Main Committee of the General Assembly entitled to verbatim records coverage."[1]

Problem Statement

The creation of the Internet launched an era of prosperity and quick communication the likes of which the world had never before seen. However, with this new development came a change in the ways in which crime and warfare were executed. With the Internet, a country can knock out the power grid of an entire major city and a criminal can hack into the bank account of someone 10,000 miles away from them. Welcome to Cybersecurity and Cyberwarfare, the topics concerning our committee. Intelligence agencies and governments everywhere are trying to both enhance their firewalls to protect against attacks and create large-scale viruses and means of attack for the purposes of either intelligence gathering, sabotage, or self-defense. Whether or not international action is needed, and what that action will be, is up to you, the delegates of your respective countries. The key aspects of this topic are cyber espionage by national governments, data theft by criminals, and arguably the fastest-growing danger, cyber-attacks meant to knock out communication, electricity, and other vital mechanics.

History

When discussing cyber-attacks and their history, we must start with the Morris worm of 1988–one of the first recognized worms to affect the world's new cyberinfrastructure, largely in the US. The worm used weaknesses in the UNIX system Noun 1 and replicated itself regularly. It slowed down computers to the point of being unusable. The worm was the work of Robert Tapan Morris, who said he was just trying to gauge how big the Internet was. He became the first person to be convicted under the the US' Computer Fraud and Abuse Act.

"The Computer Fraud and Abuse Act (CFAA) was enacted in 1986, as an amendment to the first federal computer fraud law, to address hacking. Over the years, it has been amended several times, most recently in 2008, to cover a broad range of conduct far beyond its original intent. The CFAA prohibits intentionally accessing a computer without authorization or in excess of authorization, but fails to define what "without authorization" means. With harsh penalty schemes and malleable provisions, it has become a tool ripe for abuse and use against nearly every aspect of computer activity."[2] Robert Morris now works as a professor at MIT.

The Morris Worm

When discussing cyber attacks and their history, we must start with the Morris worm of 1988–one of the first recognized worms to affect the world's new cyberinfrastructure, largely in the US. The worm used weaknesses in the UNIX system Noun 1 and replicated itself regularly. It slowed down computers to the point of being unusable. The worm was the work of Robert Tapan Morris, who said he was just trying to gauge how big the Internet was. He became the first person to be convicted under the US Computer Fraud and Abuse Act. Robert Morris now works as a professor at MIT.

"The Computer Fraud and Abuse Act (CFAA) was enacted in 1986, as an amendment to the first federal computer fraud law, to address hacking. Over the years, it has been amended several times, most recently in 2008, to cover a broad range of conduct far beyond its original intent. The CFAA prohibits intentionally accessing a computer without authorization or in excess of authorization but fails to define what 'without authorization' means. With harsh penalty schemes and malleable provisions, it has become a tool ripe for abuse and use against nearly every aspect of computer activity."

Timeline of Cyber-Related Events

December 2006

NASA blocks emails with attachments before shuttle launches out of fear they will be hacked.

Business Week reports that the plans for the latest US space launch vehicles were obtained by unknown foreign intruders.

April 2007

Estonian government networks are harassed by a denial of service attack by an unknown foreign intruders, following the country's disagreement with Russia over the removal of a war memorial. Some government online services are temporarily disrupted and online banking is halted.

The attacks aren't focused or very damaging, and the Estonians respond well, relaunching some services within hours or, at most, days.

June 2007

The US Secretary of Defense's unclassified email account is hacked by unknown foreign intruders as part of a larger series of attacks to access and exploit the Pentagon's networks.

October 2007

China's Ministry of State Security said that foreign hackers, claimed to be 42% from Taiwan and 25% from the US, had been stealing information from key Chinese areas.

In 2006, when the China Aerospace Science & Industry Corporation (CASIC) intranet network was surveyed, spyware is found in the computers of classified departments and corporate leaders.

Summer 2008

The databases of both Republican and Democratic presidential campaigns are hacked and downloaded by unknown foreign intruders.

August 2008

Computer networks in Georgia are hacked by unknown foreign intruders around the time that the country was in conflict with Russia. Graffiti appears on Georgian

government websites.

There is little to no disruption of services but the hacks put political pressure on the Georgian government and appear to be coordinated with Russian military actions.

January 2009

Hackers attack Israel's internet infrastructure during the January 2009 military offensive in the Gaza Strip. The attack, which focused on government websites, was executed by at least 5,000,000 computers.

Israeli officials believe the attack was carried out by a criminal organization based in a former Soviet state and paid for by Hamas or Hezbollah.

January 2010

A group named the "Iranian Cyber Army" disrupt the service of the popular Chinese search engine Baidu. Users are redirected to a page showing an Iranian political message.

The same "Iranian Cyber Army" had hacked into Twitter the previous December, with a similar message.

October 2010

Stuxnet, a complex piece of malware designed to interfere with Siemens industrial control systems, is discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyberweapon aimed at the Iranian nuclear program.

January 2011

The Canadian government reports a major cyber attack against its agencies, including Defence Research and Development Canada, a research agency for Canada's Department of National Defence.

The attack forces the Finance Department and Treasury Board, Canada's main economic agencies, to disconnect from the Internet.

July 2011

In a speech unveiling the Department of Defense's cyber strategy, the US Deputy Secretary of Defense mentions that a defense contractor has been hacked and 24,000 files from the Department of Defense were stolen.

October 2012

The Russian firm Kaspersky discovers a worldwide cyber-attack dubbed "Red October," that had been operating since at least 2007.

Hackers gathered information through vulnerabilities in Microsoft's Word and Excel programs. The primary targets of the attack appear to be countries in Eastern Europe, the former USSR, and Central Asia, although Western Europe and North America reported victims as well.

The virus collected information from government embassies, research firms, military installations, energy providers, nuclear and other critical infrastructures.

March 2013

South Korean financial institutions as well as the Korean broadcaster YTN have their networks infected in an incident said to resemble past cyber efforts by North Korea.

June 2013

In their first-ever meeting dedicated to cyber defense, NATO Defence Ministers agree that the Alliance's cyber-defense capability should be fully operational by the autumn, extending protection to all the networks owned and operated by the Alliance.

October 2013

The NATO Computer Incident Response Capability (NCIRC) upgrade project, a 58 Million euro improvement of NATO cyber defenses, is completed by the end of October 2013. This major capability milestone will help NATO to better protect its networks from the increasing number of cyberattacks against the Alliance's information

December 2016

On December 9, 2016, the CIA told U.S. legislators the U.S. Intelligence Community had concluded that Russia was responsible for cyberattacks during the 2016 U.S. election which helped Donald Trump win the presidency. Multiple U.S. intelligence agencies found that specific individuals tied to the Russian government provided WikiLeaks with stolen emails from the Democratic National Committee (DNC), as well as stolen emails from Hillary Clinton's campaign chairman, who was also the target of a cyberattack. These intelligence organizations additionally concluded Russia hacked the Republican National Committee (RNC) as well as the DNC, but chose not to leak information obtained from the RNC.

International Action

There has been some international cooperation around preventing and responding to cybercrime. There have been a handful of treaties agreed to by different international bodies in order to address the problems DISEC faces today. A good example is the Convention on Cybercrime in 2013 in Budapest, Hungry, which led to the ratification of an international treaty to produce more effective and cooperative laws regarding cyber-crime. You can read the treaty here in the citations and further reading section.[3]

The UN has also stated its commitment to this issue as an international body, writing:

"With the increasing proliferation of information and communication technologies (ICTs) and the growing opportunity for real-time borderless exchange, cybersecurity is a complex transnational issue that requires global cooperation for ensuring a safe Internet." According to a 2011 Norton study, threats to cyberspace have increased dramatically in the past year afflicting 431 million adult victims globally – or 14 adult victims every second, one million cybercrime victims every day.

"Cybercrime has now become a business which exceeds a trillion dollars a year in online fraud, identity theft, and lost intellectual property, affecting millions of people around the world, as well as countless businesses and governments of every nation.

To address the issues and challenges around cybersecurity and cybercrime, the United Nations Economic and Social Council (ECOSOC) held a Special Event on "Cybersecurity and Development", organized jointly by the Department of Economic and Social Affairs (DESA) and the International Telecommunication Union (ITU) on December 9th in New York.

Chaired by the President of ECOSOC, with the participation of the Secretary-General of the ITU and the Chair of the United Nations Commission on Science and Technology for Development, the special event brought together Member States, the United Nations system, the public and private sector, as well as other civil society organizations interested in the areas of cybersecurity and cybercrime.

The plenary and panel discussion aimed to (1) build awareness at the international policy level by providing ECOSOC Members with a picture of the current situation and challenges concerning cybersecurity and its links to development; (2) identify a range of best practice policies and initiatives in place around the world to build a culture of cybersecurity; and (3) explore options for a global response to rising cybercrime."[4]

Each representative on the panel discussed the multifaceted issues surrounding cybersecurity, and the necessity for member states, the private sector, civil society organizations, and law enforcement agencies to work together to manage the risks of our increasing interconnectivity.

Speakers discussed the role of economic disparities between nations and the fact that developing countries do not have the ability to combat cyber attacks and cybercrime, and its global threat to cyber peace. The lack of partnership between developed and developing countries could create "safe havens" where cyber criminals make use of legal loopholes and the lack of strong security measures to commit cybercrimes in some developing countries .

You can find other UN resolutions on Cyber-Activities in further reading/citations.[5]

Drawing attention to the challenges of protecting children online, Ms. Deborah Taylor Tate, ITU Special Envoy and Laureate for Child Online Protection encouraged parents, community leaders, and governments to access the media literacy guidelines provided online by ITU.

During the interactive session, the panelists and responding member states discussed the need for a future global convention to develop strategies, including the possibility of building upon the Budapest Convention, an international treaty seeking to align national criminal laws around computer crimes such as copyright infringement, fraud, child pornography, hate crimes, and breaches of network security.

In his concluding remarks, President of ECOSOC, H.E. Mr. Lazarous Kapambwe said, "We have agreed that cybersecurity is a global issue that can only be solved through global partnership. It affects all of our organizations…and the United Nations is positioned to bring its strategic and analytic capabilities to address these issues."

Bloc Positions

The United States, the United Kingdom, Australia, Canada, and the vast majority of NATO support improved regulation of cyberspace. These nations would like to protect freedom of information movement and are in favor of granting greater access to US and NATO-linked intelligence. These countries condemn the use cyber-attacks to further political ends, but maintain that cyber-defence also involves some level of offensive capability. They'd likely wish to see stronger firewalls and international

cooperation in handling the issue.

Russia, China, Germany, Turkey, India, Brazil, and other nations who favor national sovereignty call for regionalized cyberspace where nations have control over their own laws and act independently. They believe this will make threat detection easier. They are generally in favor of weak international action on the issue.

Estonia, Georgia, Ukraine, South Korea, Saudi Arabia and Iran are often victims of cyber attacks from regional enemies and consider cyber defence an urgent matter. They support strong international regulations to stop what others have termed cyber aggression, but they see as cyber warfare.

Specific EU and ASEAN nations like Japan, Philippines, and Malaysia see cyber security as something that should be debated before the international body but with solutions focused on the regional level, looking towards sovereignty and international consensus. Their proposals will likely try to strike a balance between the region and the international community through regional action and with international coordination.

Topics for Further Research

1. How do we stop cycles of counter attacks and attribution for previous attacks?
2. Who is responsible for enhancing cybersecurity? What resources and funds should they have, and how will those resources and funds be raised?
3. Should protection against cyber attacks be an international project or a national one?
4. How can countries coordinate to fight cybercrime?

Sources for Further Research

1. https://www.infosecurity-magazine.com/news/saudi-aramco-cyber-attacks-a-wake-up-call-says/
2. https://www.atlanticcouncil.org/news/press-releases/tallinn-manual-2-0-clarifies-how-international-law-applies-to-cyber-operations/
3. https://indianexpress.com/article/technology/tech-news-technology/petya-ransomware-cyberattack-hit-india-asia-mumbais-jawaharlal-nehru-port-

impacted-global-firms-impacted-4725599/

4. http://www.strifeblog.org/2015/08/28/cyber-risks-to-governance-part-ii-the-attribution-game-the-challenges-and-opportunities-of-cyber-attribution-in-policymaking/
5. http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
6. https://www.eu2017.ee/news/press-releases/estonia-conduct-first-cyber-defence-exercise-defence-ministers
7. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
8. https://www.theregister.co.uk/2016/01/27/ukraine_blackenergy_analysis/?page=2
9. https://kunstkritikk.com/the-reinvention-of-cyberspace/
10. https://www.bbc.com/news/39655415
11. https://www.techrepublic.com/article/cyberwar-the-smart-persons-guide/
12. https://www.vice.com/en_us/article/ezpaaz/policy-directive-41-cyber-incidents
13. https://www.nytimes.com/2017/01/06/us/politics/donald-trump-wall-hack-russia.html
14. http://jcie.org/researchpdfs/ASEAN-Japan/NavChange/9.pdf
15. http://www.washingtonpost.com/wp-dyn/content/article/2010/01/15/AR2010011503917.html
16. https://www.nytimes.com/2017/01/06/us/politics/donald-trump-wall-hack-russia.html
17. https://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939?journalCode=f
18. https://www.us-cert.gov/ncas/tips/ST04-015
19. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan
20. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Endnotes

1 "Disarmament and International Security (First Committee)," United Nations, accessed December 26, 2019, https://www.un.org/en/ga/first/

2 "Computer Fraud and Abuse Act (CFAA)," NACDL, accessed December 26, 2019, https://www.nacdl.org/Landing/ComputerFraudandAbuseAct

3 Council of Europe, *Convention on Cybercrime*. ETS No. 185, Budapest, 2004, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (accessed December 26, 2019)

4 "Cybersecurity: A global issue demanding a global approach," United Nations, accessed December 26, 2019, https://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html

5 "UN Resolutions Related to Cybersecurity," International Telecommunication Union, accessed December 26, 2019, https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx


COMMUN