Israel National Defense College
47th Class 2019-2020

Foundations of National Security in Global Perspective

Final Assignment

Lecturer: Dr. Anat Stern

Submitted by: Wong Khiong Seng

16 Dec 2019

Question.

1. **It has been claimed that globalization threatens the status of nation state. Choose a global phenomenon (you can select a phenomenon that was discussed in the course or a different one, according to your wishes). Present it and its connection to the foundations of national security and analyze the state's ability to deal with it in light of global transformations.**

INTRODUCTION

The paper will first present the advent of cyberspace as a global phenomenon. The paper will next highlight the cyber threats to national security. The paper will then conclude with an overview on the state's approach to cyber security and the challenges it faced in formulating corresponding polices to deal with cyber threats.

ADVENT OF CYBERSPACE AS A GLOBAL PHENOMENON

The advancements and innovations in computer and communication technologies have resulted in radical improvements in information and communication capabilities. With rapid and widespread assimilation of these technologies, it continues to create many new business and social opportunities that massively scale and widely interconnect.[1] According to CISCO, by 2020, the number of devices connected to the Internet will exceed 28.5 billion, more than three times the global population, and it is projected to reach a staggering 500 billion devices by 2030.[2]

In what's called the Internet of Things, or IoT, it is growing in applications and will impact nearly every part of society, including our daily personal lives as well as national critical infrastructures. The IoT is a giant network of connected things and people, collecting

[1] Michael Nadeau, "Future Cyber Security Threats and Challenges: Are You Ready For What's Coming", CSO, 19 Sep 2017. https://www.cio.co.nz/article/627512/future-cyber-security-threats-challenges-ready-what-coming. Accessed on 29 Nov 19.

[2] Cisco Systems, "Cisco Visual Networking Index: Foreast and Trends, 2017-2022 White Paper", 27 Feb 2019, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-.Assexc11-741490.html. Accessed on 29 Nov 19.

and sharing data about the way they are used and about the environment around them. We can see its application in 'Smart Homes' through service automation, allowing, for example, to open locks (e.g., with a remote control), to shop and pay for goods (e.g. using a smartphone to shop online with an electric wallet), and to track fleet trucks on the highway and in freight yards. The IoT can also allow governments to create and integrate intelligent technical solutions that smart cities require, such as smart transportation systems, smart parking, smart buildings, and smart bridges.[3] While the advent of cyberspace has offered many opportunities and benefits, there are also security concerns related to its rapid and diverse application in an unanticipated manner.

IMPLICATIONS OF CYBER THREATS ON NATIONAL SECURITY

In a very short span of time, individuals and companies have harnessed cyberspace to create new industries, a new economic sphere, and a vibrant social space that are intertwined with everyday lives. Concurrently, individuals, subnational groups, and governments are also using cyberspace to advance their interests through malicious activities. This global phenomenon of cyberspace has presented new challenges to national security and has been inexorably pitched as the fifth domain of warfare, which even the Pentagon has recognized to be just as crucial to military operations as the other conventional domains of land, sea, air and space.[4] Cyber security breaches can range from no or limited impact to Distributed Denial of Services (DDoS), or even cyber crime such as stealing of data, identity theft. The world of cyber crime is also blurring into acts of espionage, sabotage and even warfare.[5] The greatest

[3] Panel Report, "The Transformative Effect of the Internet of Things on Business and Society", Communications of the Association for Information Systems, Jan 2019, Vol 44 Paper 5, Pg. 129-140.

[4] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy", Foreign Affairs, Sep – Oct 2010, Pg. 97 – 108.

[5] Ronald Deibert, "The Growing Dark Side of Cyberspace ", Penn State Journal of Law & International Affairs Vol 1 No.2 2012, Pg 266.

impact occurs when an intruder gains access to the supervisory control access and launches control actions that may cause catastrophic damage.[6]

Cybersecurity threats to critical infrastructure, such as power plants and transportation system, is one of the most significant strategic risks for a nation as these critical infrastructures become more highly interconnected. At a benign level, cyber attacks on them could disrupt its operations leading to economic losses. Taking it to the extreme, these cyber attacks could cripple a state on the services it provide and plunge it into chaos. In May 2017, the WannaCry ransomware attack affected over 200,000 devices and machines in 150 countries; it targeted critical infrastructures, hospitals, financial institutions and factories, resulting in estimated USD4 billion of financial losses.[7] In Dec 2015, an elaborately planned cyber attack was orchestrated efficiently by organised cybercriminals and state actors to disrupt the national power grid in Ukraine.[8] With increasing reliance on digital infrastructure for these critical infrastructures to be more efficient, the cyber security risk on it is only likely to grow.

Cyber could also be used as an asymmetric weapon. When North Korea wanted to express dissatisfaction with the US due to a movie release, it didn't attack US forces in South Korea or harass commercial ships bound for the US. Instead, it conducted a cyber attack against Sony Entertainment. While North Korea remains provocative with missile and

[6] Official website of Department of Homeland Security, https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure. Accessed on 1 Dec 19.

[7] Jonathan Berr, "WannaCry" Ransomware Attack Losses Could Reach $4 illion", CBS News, 16 May 2017, https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/, Accessed on 1 Dec 2019.

[8] Kim Zetter, "Inside the Cunning Unprecedented Hack of Ukraine's Power Grid", Wired, 3 Mar 2016. http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. Accessed on 29 Nov 2019.

nuclear tests, cyber tools give the country a way to conduct attacks or harass without escalating into physical war.[9]

Cyber insecurity also has a wider societal dimension. As the public might not be well-equipped to discern quality news from fake news, disinformation and misinformation – to be intended as unfounded news or semi-truths – worked through organized campaigns with the aim to shape national opinion, could destabilize social cohesion and affect politics.[10] When news is perceived and accepted as true on the basis of emotions and sensations without any concrete analysis of its foundation, personal convictions are more influential in shaping public opinion than the objective facts. For example, in 2014, Crimea was annexed by Russian and the spread of propaganda and the manipulation of facts by Russia on Crimea people was identified to have been a significant factor. In the findings of the Senate Intelligence Committee's investigation of Russian meddling in the 2016 US presidential Election, an assessment was made which pointed to Russia's involved attacks on U.S. election infrastructure, and manipulation of social media outlets as part of a stealthy campaign to sow division among the American electorate in an effort to vault then-candidate Donald Trump into the Oval Office.

RESPONDING TO THE THREAT OF CYBERSPACE

At the state level, most nations have set up dedicated organizational structure to deal with cyber security. For example, in Singapore, the Cyber Security Agency of Singapore (CSA) was formed in 2015 as the central agency to oversee and coordinate all aspects of

[9] Derek Reveron, "How Cyberspace is Transforming International Security", Harvard Extension School, https://www.extension.harvard.edu/inside-extension/how-cyberspace-transforming-international-security. Accessed on 1 Dec 2019.

[10] Ilaria Lezzi, Fake News and National Security:Re-build trusts nad social resiience in the Post-truth era", 11 Feb 2018, http://www.medialaws.eu/fake-news-and-national-security-re-build-trust-and-social-resilience-in-the-post-truth-era/. Accessed on 1 Dec 2019.

cybersecurity for the nation. CSA is empowered to develop and enforce cybersecurity regulations, policies, and practices. In the US, the United States Cyber Command, in 2017, was elevated to the status of a Unified Combatant Command to improve its focus on cyberspace operations. These agencies would need to put in place a governance framework to help them better understand their cyber security risks and to establish policies, guidelines and standards to manage these risks. As cyberspace has continued to expand beyond national borders, cybersecurity breaches might not be stopped at a nation's borders. In fact, it is difficult to determine where the actual borders are in cyberspace.[11] Hence, it is important for nations to also establish international cooperation mechanisms and also engage in mutual assistance in the field of cyber security to respond to and limit cyber attacks.

In many states, most cybersecurity expertise lies across industry sectors and academic disciplines. Cooperation between public authorities and the private sector is therefore essential for strengthening overall levels of cybersecurity where the industry experts, academics, and the public sectors come together collectively to develop cyber security strategies to deal with cyber threats to national critical infrastructure. Governments can also launch programs for training and educating the IT workforce of public and private sector so as to raise individual awareness on cyber security. Better public awareness could lead to positive individual cyber hygiene and contribute to the prevention of cyber theft and malicious activities in the internet.

Cyberspace in national security also raises interesting questions about the role of the national government in protecting the civilian space. At the societal level, there are all sorts of civil liberties at play and the challenge of government when dealing with cyber security is

[11] Hans de Bruijn, Marijn Janssen, "Building Cybesecurity Awareness: The Need for Evidence-based Framing Strategies", Government Information Quarterly 34 (2017) 1-7, Pg 3-4.

balancing the citizens' demands and its obligations to protect national security without compromising the ability of citizens to maintain their privacy.[12] The core challenge is to frame a sustainable balance between freedom of information and national security within the domain of law. If truth is indispensable for effective decision-making, fact-based policies are essential for human progress[13] Trust and social resilience building therefore becomes one of the key factors as a response against disinformation and misinformation.

SUMMING UP

The advent of cyberspace as a global phenomenon has offered many opportunities while at the same time presented vulnerabilities to national security that would need to be dealt with. It is thus crucial that each nation build a strong national cyber system that is resilient. There is also now greater consensus that the fight against cyber threat cannot be fought alone by states and international cooperation would be needed.

BIBLIOGRAPHY

1. Michael Nadeau, "Future Cyber Security Threats and Challenges: Are You Ready For What's Coming", CSO, 19 Sep 2017. https://www.cio.co.nz/article/627512/future-cyber-security-threats-challenges-ready-what-coming. Accessed on 29 Nov 19.
2. Cisco Systems, "Cisco Visual Networking Index: Foreast and Trends, 2017-2022 White Paper", 27 Feb 2019, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-. Assexc11-741490.html. Accessed on 29 Nov 19.

[12] Derek Reveron, "How Cyberspace is Transforming International Security", Harvard Extension School, https://www.extension.harvard.edu/inside-extension/how-cyberspace-transforming-international-security, Accessed on 1 Dec 2019.

[13] Ilaria Lezzi, Fake News and National Security: Re-build trusts and Social Resilience in the Post-truth era", 11 Feb 2018, http://www.medialaws.eu/fake-news-and-national-security-re-build-trust-and-social-resilience-in-the-post-truth-era/. Accessed on 1 Dec 2019.

3. Panel Report, “The Transformative Effect of the Internet of Things on Business and Society”, Communications of the Association for Information Systems, Jan 2019, Vol 44 Paper 5, Pg. 129-140.
4. William J. Lynn III, “Defending a New Domain: The Pentagon’s Cyberstrategy”, Foreign Affairs, Sep – Oct 2010, Pg. 97 – 108.
5. Ronald Deibert, “The Growing Dark Side of Cyberspace “, Penn State Journal of Law & International Affairs Vol 1 No.2 2012, Pg 266.
6. Official website of Department of Homeland Security, https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure. Accessed on 1 Dec 19.
7. Jonathan Berr, “WannaCry” Ransomware Attack Losses Could Reach $4 illion”, CBS News, 16 May 2017, https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/, Accessed on 1 Dec 2019.
8. Kim Zetter, “Inside the Cunning Unprecedented Hack of Ukraine’s Power Grid”, Wired, 3 Mar 2016. http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. Accessed on 29 Nov 2019.
9. Derek Reveron, “How Cyberspace is Transforming International Security”, Harvard Extension School, https://www.extension.harvard.edu/inside-extension/how-cyberspace-transforming-international-security. Accessed on 1 Dec 2019.
10. Ilaria Lezzi, Fake News and National Security:Re-build trusts nad social resiience in the Post-truth era”, 11 Feb 2018, http://www.medialaws.eu/fake-news-and-national-security-re-build-trust-and-social-resilience-in-the-post-truth-era/. Accessed on 1 Dec 2019.
11. Hans de Bruijn, Marijn Janssen, “Building Cybesecurity Awareness: The Need for Evidence-based Framing Strategies”, Government Information Quarterly 34 (2017) 1-7, Pg 3-4.