THE HOUR OF CYBER SECURITY

A Paper

Presented to

Dr. Mark Caleb Smith

Cedarville University

In Partial Fulfillment

of the Requirements for POLS-3100

---

by

Rufus Roby Mathew

December 9th, 2021

Why should you be worried about your cyber data and its security? This essay exposes the threats of cyber security and proposes some solutions to counter cyber terrorism through an educated mind. It is terrifying to think that one in three Americans are a victim of cybercrime almost every year. Throughout this paper, there are many expert findings on cyber security and solutions to cyber threats. There are two levels of cyber security: the micro-level which is usually an individual's personal data. And then there is the macro level which deals with the national infrastructures like nuclear submarines, power grids, etc. The deadliest aspect of cyber threats is that people don't care, and they don't understand how their data could be used against them. As D. Perkins tries to convey in his article, Evolution of Different Dual-use Concepts, Cyber Security is protecting and respecting the rights of everyone. There are many blurred lines in cyber security as cyberspace is dynamic and fast-evolving. Cyberspace is constantly changing for the good, but along with this change, there are also new threats that evolve. The biggest blessing for cybercriminals is that people do not understand how cyberspace works! Cyberwarfare is an entirely new ball game, and we need to treat it in a different style with new weapons (p. 2).

Micro-level cyber threats are those that attack a person's data and affect their family and community. This can happen in various forms like stealing their credit card information and trying to steal their money digitally. They can even use the person's data to destroy the individual's credit score making them unable to apply for a loan to buy a house or car. Identity theft is also a very serious cyber threat. Attackers can use an individual's information to create profiles that look like their actual profile. They can use this for further fraud or post something vulgar hence destroying or creating confusion around the individual's reputation. Sometimes this

can even lead to extortion: there have been so many instances when attackers take control over a person's account and demand money to release the account and its data.

Macro-level cyber threats are those that attack the nation's assets like power grids, nuclear submarines, etc. These are generally taken up by the national Cyber command. There are many rogue nations and terrorist organizations that are trying to attack and cripple our nation constantly. They can do this in various fashions: by taking out NYC's power grid or by taking control of one nuclear silo, or even just by sending in junk data into wall street computer servers corrupting the financial world.

The attack on Sony Inc. is a good example of a recent cyber-attack that could have been avoided. In April 2011, Sony's PlayStation Network was attacked. The banking information of tens of thousands of players was also compromised. Hackers used a well-known network vulnerability that Sony chose to ignore. Unfortunately, in November 2014 Sony Pictures Entertainment was attacked by another malware. Confidential information such as film scripts, compromising emails, and personal data of 47 000 employees (names, addresses, emails, social insurance numbers, salaries, etc. Sony Pictures had carried out an audit of its security system a few months prior to the incident, and this audit had revealed serious failures in the infrastructure management, including a firewall and several hundred terminals (routers and servers) that were not managed by competent teams. But they chose to ignore it. They did not understand how open they were to cyber-attacks. Even when they were attacked the first time, they did not take any measures to prevent them from being attacked again. The fact is that if Sony can be taken down with such ease, none of our online profiles is safe either. We all have a huge online footprint in this generation. We are all ready to grab the next shiny thing like an Amazon Echo or a

self-driving car that is connected to the internet. The world loves convenience, so we grab the next big thing in the market to make our lives easier. By doing this, we are leaving ourselves open to scores of data vulnerabilities. Whenever you connect to a public WIFI, your data goes through some unsecured servers where your data can be stolen. Think about the last time you went to a coffee shop and tried to connect to their WIFI. Most coffee networks will warn you that you are entering public Wi-Fi. But we choose to ignore this message and connect to the WIFI and enter our password on this unsecured network. An anti-social element can easily connect to this WIFI and hack into the devices or servers. This is just one of the very basic examples of how we can be hacked just because of our ignorance. We are all naive when it comes to data protection. This is because of the low priority we have given to cyber security education. We are all super quick to connect to the next WIFI network without thinking of the consequences. This is a huge problem in communities, as it is not only that people are spending more time in the virtual world, but it also gives the hacker multiple fronts to attack! The biggest problem is that people think they know the virtual world more than the real world. This leaves them completely defenseless! Cyber-attacks are not only attacking your personal data, but the nation is under attack too. This can be in the form of cyber-attacks against our power grids or even by manipulating people's opinions in elections!

As Myriam Cavelty warns us in her paper, Breaking the cybersecurity dilemma, Cyber-threats, and the measures necessary to counter them are the security issues of the hour. In recent years, several sophisticated cyber-attacks and intensifying media attention have combined to give the impression that cyber-incidents are becoming more frequent, more organized, more costly, and altogether more dangerous. Politically it can have huge repercussions. The 2016 election is the

best example of this! It is scary to think that a foreign government could have influenced us to vote in their favor directly or indirectly. We have been discussing this election result for more than two years now and still do not know what has happened. This is good evidence about the difficulty in finding the culprits in online crime. This is also a great example of the difference between cyber warfare from other warfare. Any other warfare is very evident and immediately destructive. Hence, they can be tracked and defended ahead of time. But cyber-attacks are sneaky and sometimes it takes us years to detect that we have been attacked. This is the reason we need to prioritize cyber defense in our personal and nation's planning and budgeting.

A huge argument made in 'Evolution of different dual-use concepts' by J. Rath is the difference between human security and national security. Human security is people's personal safety. Citizens need to feel safe in their homes and society. This is achieved by having strong institutions like the police department, good justice missions, and an unbiased judicial system. As I mentioned earlier, cyberspace has very blurry laws, but it is in the interest of all people to keep the nation safe. National security organizations help us do that. They have strict laws and loopholes that give them the right to keep a watch on a citizen's online profile. The depth of the ability that these organizations must keep a watch on us is incredible. There is a very strong opposition that believes the government should not have the ability to keep such a close watch on the citizens. There is a huge privacy threat reason that the citizens state. We need to organize the cyber bureaucracy so that police and security services can easily use the cyber-surveillance system. Most cyber crimes have a strict time frame, so we need to ensure the bureaucracy is as effective and efficient as possible. But at the same time, we need to secure the surveillance system so that they are not used for anything illegal. This can be achieved by having random

checks into recent surveillance conducted and confirming that they have been used for the right reasons. Finding a balance between smooth bureaucracy and legitimate surveillance systems is the biggest challenge the government needs to solve. J. Rath finally proposes that the government should inform the people that the national security organizations and other branches do not encroach upon the privacy rights of the citizens. And the citizens need to understand the importance of having strong and truthful institutions that can access and monitor suspicious online profiles to keep the nation and its citizens safe.

When it comes to the nation's cyber defense, there is a huge push to start developing cyber security laws. The biggest concern of the 21st century is privacy and data protection. Since the dawn of the last century, the world has seen an increase in the digital footprint of the private sector. What is the private sector? The private sector is an organization that is privately owned and has extensive control over your digital data. Companies like Facebook, Google, Snapchat are some examples of private sector companies. When you sign into these companies, they will ask you to sign some documents that basically give them complete access to your digital data. The Cambridge analytics that caused a huge uproar against these giant companies helped create more awareness among the citizens about how their data is being used by these companies. The public sector is the government and its subsidiary organizations like the NSA, CIA, FBI. The question is how much collaboration between the private and public sectors is acceptable. This is where new cyber laws are important. Asha M. George in her research about the national security implications of cyber biosecurity talk about updating the cyber security laws. Currently, we have laws that have been in place since 1988. For an area that is literally constantly developing we need to be more prepared and attentive to the needs of the market. The good news is that this law

has been very broad, so it is still applicable to most cyber security areas. But we need new laws and competent lawyers who understand the technical details and the laws of national security. Another important step we need to take is to form an international cyber security alliance. Since cyber-attacks are mostly remote and done from another part of the world, we need a strong international organization that brings together the different nation's cyber commands. Organizations like the world bank, international court of justice function that same way in their own respective fields. Having an international cyber command helps different nations to communicate with each other faster and more effectively. This will help us catch the culprits early on no matter where they are and protect our nation.

According to the journalist Brent Cooper, Cybercrimes will cost businesses over $2 trillion total in 2019 but 95% of all cybercrimes are a result of human ignorance (p. 3). Cyber security must be given importance and discussed on national television, in schools, and even in families. It is very scary to think that because of our ignorance our family can be hurt. We need to use our biggest weapon effectively: education. We need to be discerning and stop before connecting or buying something new to our online profile. We need better cyber laws which mean we prioritize cyber warfare in our next planning and budgeting, nationally and locally. We also need stronger national and international organizations that can communicate with each other better and more efficiently. Cyber threats are scary and powerful, but the good news is that an educated mind will be much more aware and cautious. Hence protecting their personal digital data and the nation's cyber interests.

Bibliography

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. ***Science and Engineering Ethics, 20*****(3), 701-715. doi:10.1007/s11948-014-9551-y [doi]**

Dunn Cavelty does a great job of introducing cyber security to the reader. He states that people tend to neglect Cyber Security as they don't see any apparent damage to their property or life. But Cyberspace has the power to destroy information systems and take down many important infrastructures of the country. This can lead to mass confusion, chaos, and strike. It is in fact this ignorance of Cybersecurity that makes it a deadly weapon. Cavalry further goes on to talk about the importance of multidimensional and international interaction to curb cybercrimes and catch the culprits.

George, A. M. (2019). The national security implications of cyber biosecurity. ***Frontiers in Bioengineering and Biotechnology, 7*****, 51. doi:10.3389/fbioe.2019.00051 [Doi]**

Mrs. George takes us through the importance of Cybersecurity in various fields like biology or natural science. The world has complete potential to change itself using cyber biosecurity. But this also possesses the gravest cyber threats of all time! She talks about introducing a voluntary cyber biosecurity standard. This can help each country be accountable as to how they perform and hence secure themselves better. We must also include the private sector and join hands with them to protect our data. One of the major problems Mrs. George mentions is the poor funding that cyber security research gets. We need to empower them financially and with smart manpower.

Rath, J., Ischi, M., & Perkins, D. (2014). Evolution of different dual-use concepts in international and national law and its implications on research ethics and governance. ***Science and Engineering Ethics, 20*****(3), 769-790. doi:10.1007/s11948-014-9519-y [Doi]**

This paper is a wonderful collaboration between UN officials and academicians. The paper provides a good insight into the workings of international and national anti-terrorism laws. Like any free space

or opportunity zone in the world, we need to have a system to keep cybercrimes in check. Cybercrime is a new field and people are trying to study the laws that would govern cyberspace. Before placing in the safety measures and methods to catch cybercrime we need a clear law book that is standardized on an international scale. We have examples of such specific laws that came up under the United Nations Security Council Resolutions that focused on Chemical and Biological Terrorism. And we should not consider cyber terrorism any less lethal.

Spooked by cybercrime? You should be, Brent Cooper, Community Recorder guest columnist, Retrieved October 25th, 2019.

This is a column that talks about Northern Kentucky University's new cyber security division. They have a new installation of a cyber security complex that will be used to increase awareness among students about cyber security through risk management, information systems, and compliance measures. Education and awareness are key to stopping cyber security in its tracks and helping people defend themselves. Unlike most warfare or terrorism, cybercrimes do not involve big lights, sound, or any warning. They are quiet, quick, and mostly target a very specific region, enterprise, or individual. This is the reason people are tier-1 cyber security personnel to protect their data. We need now than ever before for individuals to be equipped to handle the warfare themselves and fend off the hackers to a great extent.

WG. Nikhita Reddy, G.J Ugander Reddy. A study of cyber security challenges and its emerging trends on latest technologies, Retrieved October 25th, 2019.

A study of cyber security has shown that most hackers share their malware/ phishing techniques on the internet. The unfortunate part is that most of the platforms that they use to share the malware are legal and legitimate services. This raises huge concerns about the data that is being shared over such productive platforms. One of the biggest questions that can be raised here is privacy and whether the government has the right to

peek into citizen's internet life. This will be a big debate over the next few years as governments try to curb the cyber breaches and try to keep their citizens and systems safe.

Wu, G., Sun, J., & Chen, J. (2018). Optimal data injection attacks in cyber-physical systems. *IEEE Transactions on Cybernetics, 48*(12), 3302-3312. doi:10.1109/TCYB.2018.2846365 [doi]

Data manipulation is one of the biggest concerns for all cyber security officials. If an attacker introduces junk data in the system using the open network the algorithms will crash. Most systems in the world are digitally operated now from military satellites to autopilots in airplanes. Almost every aspect of human life is now some way or the other under the threat of cybercrime. And because these systems do wide-ranging powerful functions, even the simplest of them have thousands of input variations. An attacker could easily manipulate the access information and input junk data into the system and destroy the machine. Imagine the devastating situation if the temperature controlling system in a nuclear power plant had the wrong data. Therefore, it is very important to have secure lines of communication within a highly secure sector.