# Social Meaning and Impact of Cybersecurity-Related Technical Systems

Alexander Bonhomme

School of Cybersecurity, Old Dominion University

CYSE200T: Cybersecurity, Technology & Society

Professor Chris Bowman

April 23, 2022

# Social Meaning and Impact of Cybersecurity-Related Technical Systems

Throughout the years, technology has developed vastly, at a very swift rate. It has been incorporated into our everyday lives to the point where many people don't even know how it is implemented since it is so common. With this commonality of technology in our lives, the public also wouldn't think on how they are impacted by it, or how there are cybersecurity programs in place to keep us safe from adversaries, or those with malicious intent toward others with computer systems. As with any good thing, there is a bad side to technology in how people use it, aka those with a lack of morality or ethics (adversaries). There are plenty of attacks daily that allow for the exploitation of computer systems, and these are combatted with said cybersecurity systems in place. To account for the impact these systems have on our daily lives, we should consider the ethics behind these cyber systems, the cyber threats and cybersecurity that impact all of society, and the information systems security frameworks.

## Ethics

While there are many interpretations, ethics are simply the moral principles that govern how people make decisions and lead their lives (BBC, 2014). For those who don't think about technology's impact on society, one might believe that there is no ethical implication on using technology or the growth of technology. On the contrary, a psychologist by the name of Hans Jonas led a discussion on this relationship between ethical frameworks and technology (Jonas, 2014). In this discussion, Jonas enlightened his audience on how technology has changed human nature in how lifestyles and morals have changed for the worse. Here, modern technology is said to have brought forth new ideologies that cannot be formatted in traditional ethical frameworks.

In our daily lives, I believe that there is not an issue with the growth of technology, but within individual morals.

While there are some ethical issues that are closely connected to technology, such as trust, knowledge, and privacy, these issues arise with human use. In a natural sense, there are ethical issues with the use of just about any device, technological or not, because of dangerous possibilities. Just as there are stipulations regarding the use of a knife to cut groceries vs killing someone, the use of technology is more relevant versus the growth of technology when regarding ethical aspects. With this growth, however, there are stipulations with people who can either steal devices, or information from devices. Hacking, for example is an obvious ethical issue that arises with not only the use of technology, but human association and malicious thinking behind it. I do not agree with the writer in that Hans Jonas believes that the growth of technology has caused a need for completely new ethical laws and implications as this growth has bypassed the traditional ethical framework. Now as the growth of technology has surpassed this framework, it still falls under traditional ethical concepts. There may be some improvements made to encompass as many technological advances as possible, but traditional concepts can be and are still applied.

## Cyber Threats

In computing security, cyber threats are potential actions with malicious intent to exploit a vulnerability that results in an unwanted impact to a computer system. As shown in "Electric Grid Security and Resilience"(Energy.gov, 2016), connectivity of the North American power grid is stretching directly into homes and businesses of customers. As this does have many benefits, such as improving energy efficiency, it may be seen as easily exploitable in the eyes of those with malicious intent. With the growth of technology in our society, the types of malicious cyber-related activities that the grid is now prone to includes hacking, malicious code, loss of intellectual property, phishing, denial of service, and insider damage. Hacking is essentially the espionage and/or theft of intellectual data.

Now there are different types of hackers that are split up into groups. The different types of hackers include white hat, black hat, as well as grey, red, green, etc. White hat hackers are authorized hackers under a corporation. These hackers may also hack their own companies in order to find vulnerabilities to help bolster cybersecurity. Black hat hackers are criminal hackers that hack for their own benefit (or for the benefit of someone who pays them) to steal intellectual data. You will see these types of hackers in radical groups that are dangerous to companies with targeted intellectual data and the power grid. Grey hat hackers are none of the above, just cybersecurity experts who hack without malicious intent. No data is ever stolen with them, but they just like to find gaps in computer systems without the owner's permission. According to pandasecurity.com, red hats are government-hired hackers who sometimes specify in disarming black-hat hackers. These hackers use tactics that black hat hackers use and turn it against them. There are also other types such as script-kiddies and blue hats, and they all perform somewhat different duties. Even in just hacking, it is important to understand how each type of malicious hacker can implement cyber-attacks, thus using non-malicious hackers to defend against it, and even counterattack.

To enlighten with some of the various ways one can be exploited besides hacking, there includes:

- **Phishing**
    - Most popular cyberattack where adversaries spam users online through e-mails pretending to be an authority figure or promising certain prizes, and to click a link

to fix the situation. Upon clicking the link, the user’s device becomes infected with viruses and sensitive data can be stolen

- **Identity Theft**
  - Stealing personal information to sell to third parties or other fraudulent purposes.
- **Denial of Service (DoS)**
  - Adversaries flood a user’s device’s network with requests causing it to crash and take it offline (ex. booting someone off a video game server)
- **Malware attacks**
  - Includes ransomware, spyware, or trojan horse, and is a broad variety of attacks to infiltrate a computer system to leave malware such as viruses or to steal sensitive information.
    - **Ransomware** stalls a computer system and locks the user out for a fee, and if the fee is paid, then the situation will be fixed (or at least that is what the user will see, the adversary does not always follow through on their “promise”.
    - **Spyware** uses software such as keylogging to record the user’s keystrokes on their keyboard, or it can be seen in remotely accessing a user’s camera to see them on the other side.
    - **Trojan Horses** are a type of malware disguised as harmless or necessary software, but once downloaded release viruses inside the system

With the many means that exist to commit cybercrime, there are also many reasons and motivations that push adversaries in that direction. According to Comparitech, 72% of cybersecurity breaches in 2019 were financially motivated while 26% were traced down to espionage. If analyzed from the underground economy, a big motivation is the exchange of illegal goods and services (in this case, sensitive data and information) for money (Cai, T et. al., 2018).

**Information Systems Security**

When dealing with cybersecurity, there are frameworks in place that break down what exactly computing security is. To discuss how these are used in everyone’s devices and lives, we will start with the information security triad, as discussed in Chapter 6 of *Information Systems for Businesses and Beyond*, 2014. The information security triad consists of Confidentiality, Integrity, and Availability. Confidentiality consists of restricting who has access to your information. Whoever has authorized access to that information are the only ones who can view said contents. Integrity is the assurance that said accessed information will not be altered or tampered with. This shows the information as it is, and as the data was initially inputted by the author. Integrity delineates that the information there is true. Information can lose integrity through malicious intent, such as hacking. The last part, Availability, regards the ability to access one's own information in a timely manner. As we see in our everyday life, there are (or rather, there should be) no bushes to beat around when attempting to access your own personal information.

To delve further into the frameworks implanted to keep people and their devices safe, more levels will be discussed such as authentication, encryption, etc. Authentication is identifying someone through certain factors, including what they know, what they have, or who they are. This is more commonly seen in logging in to accounts with a username and password (indicating what the user knows). Something they have could be a key, or card, although that can be problematic when stolen. As it has been used for monarch logins here, we have multi-factor authentication in place, using our login as well as duo mobile, a call, or a text message to make sure the student/faculty is who they say they are. Multi-factor authentication, as seen in the example, just combines two or more of the authentication methods listed above. Encryption is the process of encoding data upon its transmission/storage so only authorized persons can read it. The computer program that sends the information encodes the data; the receiver then decodes the data upon receiving it, since they share an encryption key. In case certain systems fail, or are attacked, regular backups should be put into place to lose minimal, if at all any data. A good backup plan includes full understanding of available resources, regular backups, offsite storage of backup data sets, and tests to make sure the data was fully restored. Physical security, while underrated, is the protection of hardware and networking components that store and transmit data. Regarding cybersecurity for organizations, and in general, this means locked doors, some intrusion detection system, secured equipment, environmental monitoring, and training on how to secure the equipment. Many people who rely heavily on software security tend to disregard actual physical security since it is easy to forget when one's head is wrapped up in possible cyberattacks and malware that can be implemented in a device.

## Conclusion

As technology has developed, it has been incorporated into our everyday lives to the point where many people don't even know how it is implemented since it is so common. Now although modern technology may be commonly utilized, the general public do not think on how they are impacted by it, or how there are cybersecurity programs in place to keep us safe from adversaries. Those with malicious intent toward others with computer systems are not on their minds as they scroll through social media and the internet. As with any good thing, there is a bad side to technology in how people use it, aka those with a lack of morality or ethics (adversaries).

There are plenty of attacks daily that allow for the exploitation of computer systems, and these are combatted with said cybersecurity systems in place. To account for the impact these systems have on our daily lives, we should consider the ethics behind these cyber systems, the cyber threats and cybersecurity that impact all of society, and the information systems security frameworks.

# Works Cited

BBC. “Ethics - Introduction to Ethics: Ethics: A General Introduction.” *BBC*, BBC, https://www.bbc.co.uk/ethics/introduction/intro_1.shtml.

Bourgeois, David. “Chapter 6: Information Systems Security - CPP.” *Information Systems for Businesses and Beyond*, 2014, https://www.cpp.edu/~raguthrie/CIS310/ISBB/Chapter6_InformationSystemsSecurity.pdf.

Cai, T, et al. “Characteristics of Cybercrimes: Evidence from Chinese Judgment Documents.” *Taylor & Francis*, https://www.tandfonline.com/doi/full/10.1080/15614263.2018.1507895.

“Electric Grid Security and Resilience - Energy.” *Energy.gov*, 2016, https://www.energy.gov/sites/prod/files/2017/01/f34/Electric%20Grid%20Security%20and%20Resilience--Establishing%20a%20Baseline%20for%20Adversarial%20Threats.pdf.

Jonas, Hans. “14B - Jonas - Tech Responsibility Reflections.pdf.” *Google Drive*, Google, 2014, https://drive.google.com/file/d/17plbz5CqnnlbubcTfgMBUHEQMAjDQ3DB/view.

Zaharia, Andra, et al. “300+ Terrifying Cybercrime & Cybersecurity Statistics (2022).” *Comparitech*, 12 Apr. 2022, https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/.