Cybersecurity Education and the Modern Dependence on ICTs

CYSE 200T – 27647

John Ryan

April 23, 2023

Introduction

Information and communication technologies (ICTs) have gained a level of sophistication and ubiquity, changing the relationship between humans and their environment dramatically. This evolution has resulted in a greater dependence on these systems for the modern workings of society. Governance itself, the means through which this dependence would historically have been managed, is also changing, with a devolution of power to non-state actors. This fact and the gap between technical knowledge and predictive knowledge require a new ethical framework that demands education at the level of the individual.

The “informatization” of critical infrastructure management offers a demonstration of society’s dependence on ICTs. There is a need to approach further integration with an effort to understand future effects of this dependence.

The goal should be to create cyber-aware, knowledge-seeking citizens who are cognizant of their increased dependence on these systems and ethical consideration of their actions using new and powerful technologies.

Hyperhistory and the Lack of Predictive Knowledge

Floridi divides human history into three eras: prehistory, history, and hyperhistory (2015). Prehistory was the time before written knowledge transfer, or the time before any information and communication technologies (ICTs) were used. History was the time where ICTs were used, but society was not yet dependent on them. The era we are in today is that of hyperhistory, where there exists a dependence on ICTs (Floridi, 2015).

According to Floridi, today's ICTs democratize data and the processing and control of them, shifting the power dynamic and decoupling power from force (i.e. government) (2015). They also "de-territorialize" human experience, making borders less relevant. Finally, the effect of ICTs on organization changes political topology, allowing faster group formation and breakup (Floridi, 2015).

The weakening position of the state as the only information agent has led to the emergence of dynamic multi-agent systems (MASs) (Floridi, 2015). In the political space, there are risks associated with this devolution of power. There are questions of identity and cohesion, consent, the primacy of the social space, and legitimacy (Floridi, 2015).

The era of hyperhistory is categorized by "exponential, relentless change (Floridi, 2015)." A new, paradigm-shifting technology like the Internet appears, only to be joined by the ubiquity of powerful mobile devices a few years later. Artificial intelligence, a data-driven advance following the creation of the Internet, is the most recent advance that will alter the human race's relationship with information. Each of these technologies radically alter how we interact with information and, subsequently, how we interact with each other and our environment.

The speed of technological change limits our ability to predict not only the direction of future change, but also the long-term effects of our immediate actions. Burning fossil fuels has done

much to drive economic growth and technological advancement, yet the true cost of doing so was not realized until damage on a planetary scale was already accrued. We are now faced with a pressing need to alter a system that has worked for generations, possibly to ensure the survival of the species. Who can say where applications of artificial intelligence today will lead?

Jonas claims that with the survival of humanity and the biosphere itself at risk with the pace of technological gain, no one can afford to act blindly (1973). Given long and complex cause and effect chains, knowledge acquisition becomes the prime duty. Ignorance is no longer an excuse; it is our ethical duty to work to close the gap between predictive knowledge and technical knowledge.

Critical Infrastructure

Critical infrastructure is defined as “assets, systems, and networks, whether physical or virtual, [that] are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof (CISA, n.d.).” CISA provides a list of 16 sectors meeting these criteria: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors / materials and waste, transportation, and water / wastewater (CISA, n.d.).

The critical infrastructure domains listed above are each increasingly dependent on ICTs. The energy sector is an illustrative example. The large geographical distribution of its industrial control systems requires remote access, control, and data gathering. Smart grids are extending networks into homes and businesses, further expanding the data footprint. As a result of these changes, the amount of information that needs to be processed and protected is increasing.

SCADA (Supervisory Control and Data Acquisition) systems are industrial control systems used to control infrastructure, facility-based, or industrial processes (*SCADA Systems*, n.d.). “Nearly all the control actions are automatically performed by the remote terminal units (RTUs) or by the programmable logic controllers (PLCs),” while the SCADA systems translate data from these into information that people can understand and use in decision-making. This information is fed through human machine interfaces (HMIs) where it can be viewed and sometimes acted upon through control elements (*SCADA Systems, n.d.*).

These systems serve two critical functions: 1) providing near real-time information that can be used to detect incidents, and 2) offering a means of responding to incidents. For example, if a weather event downs a power line, the resulting changes to telemetry will make it known immediately. Circuits may then be diverted to maintain services.

SCADA is a powerful tool for monitoring vulnerable assets and responding to incidents. However, these systems come with vulnerabilities of their own. As utilities become more dependent on these systems for their operations it increases the likelihood of an adverse cyber event affecting a society more dependent on access to energy than ever before.

The Human Factor in Cybersecurity

Capone argues that “while people are certainly an important aspect of data security and serve as critical administrators, they cannot serve as the be-all-end-all. Human behavior has proven that we choose to take the easy road, cut corners and make mistakes. (Capone, 2018, p 3).” In other words, people are the weakest link, even at the trusted administrator level.

Technical solutions can do things that humans cannot, like aggregate and inspect millions of logs or inspect every packet leaving the network. Tools like endpoint security system software, firewalls, SIEMs, email gateways, data loss prevention systems, and file integrity monitors work

to catch the result of what was likely a poor decision made by a human. However, even with many automated technical solutions, a human being must review their output. That individual must appreciate the importance of that process and be trained in what to look for and how to respond. Furthermore, most technical solutions are detective in nature. An antivirus scan may reveal malware, but at that point it is already on the network. Prevention should be the goal and can only be attained through routine training, given the prevalence of human fallibility as the cause of cyber events (e.g. through successful phishing attempts).

Cybersecurity education, whether in the form of focused training at the workplace, or more broadly as it relates to understanding the philosophical concerns of where we are going as a society, needs to improve. In an increasingly multi-agent political system, it is the individual who wields power, and therefore, the most responsibility. Whether it is an employee plugging a thumb drive into a work laptop or a citizen blithely feeding personal data into an AI-powered application, they need to be aware of the potential ramifications.

Conclusion

The pace of technological change will not slow. ICTs will continue to evolve in ways that cannot be easily predicted. This will change how resources are managed and how people interact with each other, their governments, and the environment. There will be new risks to society as dependence on ICTs grows across critical infrastructure sectors.

There is no way to guarantee we will not run aground on future “unknown unknowns” as technological advances march forward. Cybersecurity education can inoculate citizens against some of the unforeseen effects, however. Understanding our dependence on technology and the associated risks is a prerequisite to adjusting behavior, whether that means how one votes, buying habits, or data sharing decisions.

References

Capone, J. (2018, May 25). *The impact of human behavior on security*. CSO. https://www.csoonline.com/article/3275930/the-impact-of-human-behavior-on-security.html

Cybersecurity and Infrastructure Security Agency CISA (n.d.). *Critical Infrastructure Sectors.* *https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors*

Floridi, L. (2015). Hyperhistory and the Philosophy of Information Policies. In: Floridi, L. (eds) *The Onlife Manifesto* (pp. 51-63). Springer, Cham. https://doi.org/10.1007/978-3-319-04093-6_12

Jonas, H. (1973). Technology and Responsibility: Reflections on the New Tasks of Ethics. *Social Research, 40(1),* 31-54. http://www.jstor.org/stable/40970125

SCADA Systems (n.d.). *Retrieved March 15, 2023, from http://www.scadasystems.net*