# Cybersecurity in our World – A World of Information

James Baumhardt

Grand Valley State University

Brian R. Johnson, Ph.D.

# Cybersecurity in our World – A World of Information

There are so many different variations and layers to define what cybersecurity actually is and what it deals with. The term is largely used, and its own definitions are dependent between contexts, highly variable, subjective at times, and even uninformative given the right circumstances (Craigen, Diakun-Thibault, & Purse, 2014). Through literature review, there have been dominant themes suggested by Craigen et al. (2014) that help explain the different parts of cybersecurity. These themes are based on events, processes and methods, technological solutions, human engagement, and denotation objects of security. This paper describes different subjects that Cybersecurity covers in todays growing world.

Along with these themes, Cybersecurity has some distinguishing aspects. According to Craigen et al. (2014), cybersecurity is distinguished by its multidisciplinary social-technical character, it being a range-free network in which the potential of network actors are possibly akin, and its high amount of change involved with interactions. With these themes and distinguishing aspects settled, Craigen et al. (2014) compared internet definitions of cybersecurity side by side and created a new definition that combined all parts. Craigen et al. (2014) proposes that cybersecurity is the organization and arrangement of various elements such as resources, frameworks, structures, and procedures used to protect cyberspace and cyberspace-enabled systems against situations that misalign de facto from de jure property rights. Craigen et al. (2014) also explains that any instance or incident, whether by accident or intentional, that misaligns actual (de facto) property rights from anticipated (de jure) property rights is a cybersecurity incident. As these incidents happen more and more frequently, people can see that cybersecurity brings its own unique challenges, threats, and culture behind its doors.

As the world evolves, technology and security is continuing to grow. The digital world is inviting change in everything as billions of Internet of Things (IoT) devices are getting connected and set up through the internet. With an increasing amount of change, risks increase in correlation with that amount of change. While digitizing the economy, critical infrastructure and society brings many benefits, it creates a very productive base or launching pad for criminals to use these benefits as well and abuse them for their interests (Hussain et al., 2020). Hussain et al. (2020) also states that as people's dependency on digital technology grows, the incentive for criminals to take advantage of digital technology to cause tremendous damage grows. The areas of most importance consist of threats and challenges, cybercrimes, critical infrastructure, and cultural significance.

With new technology coming out at a rapid pace, it is hard to catch up on the latest patches due to vulnerabilities and their trends. Patches are updates to software where vulnerabilities were previously found; the patch fixes the vulnerability. Lewallen (2020) writes that new technologies have increased the quantity, type, and scope of assets vulnerable to cyberthreats. Hussain et al (2020) states that the top three emerging threats in cyberspace and digital media are cloud computing, IoT, and smartphones. All of these things are relatively new and still have a lot of problems with the benefits that they bring. These three things are not the only threats to cybersecurity, but they are the largest by far. These items have the greatest potential for exploitation due to the daily use that their users rely on, and because they are connecting to everything. Because of the rapidness in which new technologies are emerging, it is hard to predict the future in what to be prepared for (Lewallen, 2020).

When ensuring cybersecurity, there are many challenges. A big portion of those presented challenges involve governance. There are two types of governance: one, big

government, and two, governance inside an organization. For governance inside an organization, cybersecurity governance is needed. Hussian et. al (2020) says that when implementing standard and appropriate governance in an organization, many factors need to be looked at. Inadequate governance can be caused by malpractice and malfeasance such as improper or lack of enforcement, a misunderstanding or lack of accountability, lack of proper and adequate organizational infrastructure, and a lack of risk management. Hussian et al. (2020) also writes that the number one reason that poor cybersecurity and poor cybersecurity practices are allowed to happen is because there is no firm infrastructure with a flexible and sustainable framework to base judgement on. Also, political, managerial, and improper governing factors inside an organization can grow poor cybersecurity practices and undermine values of integrity.

For big government, state or federal, Lewallen (2020) firmly addresses that in order for governments to regulate, they themselves must first define the problem or situation at hand and decide which policymakers have the ought and authority to make decisions. Lewallen (2020) also firmly addresses that changing and new technologies have played a huge role in the creation and development of cybersecurity policy in the United States. New technologies have created uncertainty about which regulators and regulations government bodies will be subjected to. As new technologies are created, new policy must be written to regulate that technology because it can disrupt claims to authority and jurisdictional frameworks (Lewallen, 2020). Creating policies that keep up to date with the latest cybersecurity standards can be challenging, especially when legislatures and regulators are grasping and competing at the opportunity to be authoritative. Lewallen (2020), actually writes that this competition between legislatures and regulators over new technologies is opportunistic because it provides industries and organizations with opportunities to increase their own productivity and to favor their image to their liking. For

example, Lewallen (2020) goes on to write how Uber and Lyft, which are ridesharing companies where someone pay someone else to drive them someplace, try to portray themselves as "technology" companies instead of transportation companies in order to avoid local regulations and restrictions on labor and transportation.

Stemming from policy, the culture behind being cyber-aware has also become one of the larger issues dealing with cybersecurity. Hussian et al. (2020) writes that because of the culture behind the cyber world, human factors, which include lack of awareness, lack of acknowledgement, and the inability to adhere to policy and follow rules, is recognized and thought of as one of the most dangerous issues in and to cybersecurity and cyber-related functions. Users are thought of as the weakest link in the security chain due to their lack of awareness and insecure and particular behavior (Gcaza & Solms, 2017). Gcaza & Solms, (2017) also report that even with users who have more cybersecurity vigilance are reported to behave exactly like users who do not have any form of cybersecurity vigilance. Cybersecurity culture is delimited by concepts and can be categorized as an ill-defined problem. Building a good cyber-aware culture can help get rid of the human error factor that causes a lot of cybersecurity related incidents). Gcaza & Solms, (2017) also discusses that organizations must try to regulate and train employees to deal with cyber incidents in order to limit cybersecurity incidents. Organizations must have proper policies and procedures in case of a cybersecurity incident, and employees must be aware of this plan if it involves business continuity to bolster asset protection and limit asset loss. The only way to adhere culture to becoming better at cyber-activities is through teaching discipline.

Growing teaching discipline is not only in the organization where employees reside and do their day-to-day activities, but it is also in education. With an emerging global crisis, new and

plentiful avenues of technological reach, of online activity, the cybersecurity field is emerging at an alarming rate with the ideas of international interest and support (Parrish, 2018). Cybersecurity is becoming a true academic perspective instead of only being looked at as an organizational training platform for specialized jobs. In fact, Parrish et al. (2018) states that the drive to get more cybersecurity training and discipline is driven by providing guidance to higher education; implementing college cybersecurity programs. Education systems around the world are trying to scale up their resources and programs in order to meet the workforce demands that cyber-development and cyber-protection requires. Parrish et al. (2018) also goes on to state that the global information technology infrastructure is fragile, or perhaps brittle, and that the cost for not implementing cybersecurity programs at higher educational levels around the world will lead to society not having the capability and capacity to deal with emerging cyber challenges. It is important to have education regarding good cybersecurity habits and system management because globally, people have different opinions, thoughts, values, and principles about what cybersecurity should be.

The international discourse around the principles and values of global cybersecurity and its culture it brings is at an early stage and is important for the creation of talk between nation-state political actors regarding normal use of responsible and correct behavior in the cyberworld (Paziuk & Mitsik, 2019). In developing a good, global cybersecurity culture, we need to provide a framework that can be recognized worldwide, that protects human values as a number one core component. Paziuk & Mitsik (2019) says proof that a way to achieve this is by identifying the influencing and governing forces because of political actors; trends and predictions could be made from this point of view. Since there are, and will always be, differences in political priorities in nations around the globe, developing global cybersecurity culture is slow and

difficult. In 2003, the beginning of global cybersecurity culture, the Untied Nations General Assembly invited states to develop cybersecurity culture in their societies how they saw fit (Paziuk & Mitsil (2019).

Paziuk & Mitsil (2019) goes on to write about how the current state of international discourse regarding rules of responsible behavior of a nation-state emerged from the analysis and conclusion of the discussions that were held in the First Committee of the UN General Assembly at its 73rd session in October 2018. These discussions were given the name 'Developments in the Field of Information and Telecommunications in the context of International Security,' and have helped develop what we have for international relations regarding cyber activity (Paziuk & Mitsil (2019). Global cybersecurity culture, when it deals with states and intergovernmental organizations, is geopolitically vulnerable, ambiguous, and very important for maintaining security on the international scale. Inside of the 2018 discussions, the examples given of this thought came from the resolutions between the United States and the Russian Federation where both countries' resolutions defined the need to develop practices and standard of proper behavior in cyberspace, but each had different goals and implementation mechanisms. Since countries will implement cybersecurity programs and functions as they see fit, ethics plays a huge role in cyberactivity's.

Ethics plays a huge part in the human role in cybersecurity. In ethics education, people cannot know or be taught exactly what to do in every ethical dilemma they will encounter. Manjikian (2018) writes that there are four ethical concerns in cybersecurity that are a problem. These ethical concerns are: 1) the problem of surveillance, 2) the problem of privacy, 3) the problem of piracy, and 4) the problem of cyberwarfare. So many issues can become prominent if ethical decisions are not made and standards are not followed. In technology, there are a lot of

situations that involve grey areas, or unjust laws, where someone who is dealing with code or is a security professional, and that they have to act on their own accord to think ethically in order to do a task or lead a group of people in their organization (Manjikian, 2018). In these grey areas, there is a possibility for someone to do harm, make a mistake, or make any unethical choice that leads to issues regarding others or themselves. With these gray areas, there are a lot of prevalent issues that can correlate to conflict in the world.

One of these issues is the issue of corruption in the cyberworld. The legal control of processes that may suffer from the threat of corruption have always been prevalent and an important issue in countries and lands throughout history. Among the different cybersecurity threats in the world, corruption plays one of the most impactful roles in which it may make a protective system of a country or organization in danger of failing. It is hard to root out corruption as it can be anywhere, anytime, and by anyone. Holovkin et al. (2021) explains that there are two components in order to try and alleviate cybersecurity corruption: to make sure that an administration is educated and ideologically trained to handle people and situations regarding people, and making members of society have similar qualities to the administration. Holovkin et al. (2021) further explains that the development of a state or organization's cybersecurity program, along with the economic policy of the nation-state, is dependent on how society views its country regarding traditional and historical values, ideologies, and modern information literature as a willingness to not cause harm to itself or turn its back against its own people. If people are happy, then there is less chance that an individual might feel determined to do a corrupt act against their own people or organization. Regarding nation states, cybersecurity and corrupt actions can rise tensions globally if policy and process is deemed wrong by another nation state; nation states can influence others through cyber warfare and cyber intelligence.

Nation-states, or their subsidiary groups, have also been known to carry out cyberattacks in different countries in recent history. This can cause problems where one country or organization denies carrying out an attack, but the group did do the attack on a target. Rohith & Batth, (2019) says that cyberwarfare is like a cold war, in which both sides, or one side does things to escalate tensions when they do not do anything in direct open conflict. This can be stealing information from government or organizational assets, shutting down networks, and other bad things. Rohith & Batth, (2019) also says that when a state or organization carries out an attack on a foreign target, the motivation behind the incident is most likely political. Countries or organizations carry out cyber-attacks to achieve certain goals, which typically reflect their larger strategic goals (Geers. Kindlund, Moran, Rachwald, FireEye Labs, & FireEye Inc, 2013). Geers et al. (2013) also says that since cyber-attacks are low-cost bring high payoff, in targeting assets, critical infrastructure, and other sources, that they are and should be a national security concern. The biggest challenge to deterring a cyberattack is the problem of correctly identifying the attacker (Geers et al., 2013) People should not upset or accuse a country or organization of committing such an attack if they do not know if they actually did it. This type of decision making is vital for seeking peace.

Public policy discussions about cybersecurity is dominated by analogies to war and the Cold War. The introduction and implementation of cybersecurity and cyberattacks has changed the law of war globally. Lawson (2012) describes how close we are to conflict now with cyber-attacks because what is the cutoff point in which a foreign operated cyberattack requires the response of homeland military assets? What constitutes war in the digital era? These questions are important because countries will behave in the best interests of their country, and that may be different depending on where they are in the world. Cyberwar is trending to get more and more

common (Cetron, Davies, Steele, & Ayers, 2009). Cetron et. al (2009) shares common future trends in cyberwarfare. Trend one is that technology is taking a more dominant role in both society and the economy. Trend two is that communication technologies are changing fast and are influencing how people work and live. Trend three is that the global economic system is changing and that it is becoming more connected. Trend four is that research buildout plays a more prominent role in the global economy. The last trend, trend five, is that how with the fast pace of technology, and how useful attacks are in not killing people but causing economic impact is favorable over more conventional warfare.

In conclusion, cybersecurity plays a more important role in our lives now than ever before. Even if we do not consider it to do so, or are blind to its potential benefits and flaws, it will still affect us at every level of interaction from personal, to social, and eventually governmental. Cybersecurity has human flaws, but it also can have technical flaws. No system will ever be 100% secure, and that is why having a good cybersecurity policy and training is important. We must create a cyber-aware and disciplined culture in our societies that knows how to deal with cyber actions. There will be many more challenges that will come up and develop in the future regarding cybersecurity and its implications. We must not let people be corrupt and abuse their power for personal gain or outside influences. We are truly living in a world of information, and if we are not careful, that information can be used against us.

References

Cetron, M. J., Davies, O., Steele, S. F., & Ayers, C. E. (2009, Sep). World war 3.0: Ten critical trends for cybersecurity. The Futurist, 43, 40-49. Retrieved from http://search.proquest.com.ezproxy.gvsu.edu/magazines/world-war-3-0-ten-critical-trends-cybersecurity/docview/218565971/se-2

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. https://www.timreview.ca/article/835

Gcaza, N., & Von Solms, R. (2017). Cybersecurity Culture: an Ill-Defined Problem. In *IFIP advances in information and communication technology* (pp. 98–109). https://doi.org/10.1007/978-3-319-58553-6_9

Geers, K., Kindlund, D., Moran, N., Rachwald, R., FireEye Labs, & FireEye, Inc. (n.d.). *World War C: Understanding Nation-State motives behind today's advanced cyber attacks*. https://cyberwarzone.com/wp-content/uploads/papers/fireeye-wwc-report.pdf

Holovkin, B. M., Tavolzhanskyi, O. V., & Lysodyed, O. V. (2021). Corruption as a cybersecurity threat in conditions of the new world's order. Linguistics and Culture Review, 5(S3), 499-512. https://doi.org/10.37028/lingcure.v5nS3.1538

Hussain, A., Mohamed, A., & Razali, S. (2020). A Review on Cybersecurity: Challenges & Emerging Threats. *UiTM Cybersecurity*. https://doi.org/10.1145/3386723.3387847

Lawson, S. (2012). Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. *First Monday*. https://doi.org/10.5210/fm.v17i7.3848

Lewallen, J. (2020). Emerging technologies and problem definition uncertainty: The case of cybersecurity. *Regulation & Governance*, *15*(4), 1035–1052. https://doi.org/10.1111/rego.12341

Manjikian, M. (2017). *Cybersecurity ethics: An introduction*. *Taylor & Francis Group* (1st ed.). London: Routledge. https://doi.org/10.4324/9781315196275

Parrish, A., Impagliazzo, J., Raj, R. K., Santos, H., Asghar, M. R., Jøsang, A., . . . Stavrou, E. (2018). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. *Asd*. https://doi.org/10.1145/3293881.3295778

Paziuk, A., & Mitsik, V. (2019). GLOBAL CYBERSECURITY CULTURE IN THE INTERNATIONAL DISCOURSE: VALUES AND PRINCIPLES. https://elib.nakkkim.edu.ua/handle/123456789/2702

Rohith C. & Batth, R. S. "Cyber Warfare: Nations Cyber Conflicts, Cyber Cold War Between Nations and its Repercussion," 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 2019, pp. 640-645, doi: 10.1109/ICCIKE47802.2019.9004236.