Cybersecurity in a Changing World

Leah N. Drew

Old Dominion University

Cybersecurity is a multidisciplinary field that changes much more rapidly than others. Because we develop new technology quickly, it's difficult to predict what the future will be like. In order to overcome this issue, cyber-policy needs to be adaptable and accept technology as part of our lives rather than as an extension of it.

Changes Across Disciplines

Cybersecurity and Cyber-policy

In the past, security regulations could stay the same for decades. The way we defined morality didn't change because the world wasn't changing. That is not the case for cyber-policy. We can't predict whether the policies we develop today will be effective in the future. We certainly can't create policies and *expect* them to work in the future. Those policies will become obsolete and need replacing or updating. Our infrastructure also becomes more and more susceptible to problems as technology develops and attackers find new ways of getting around existing security systems. Because of this, I believe that cyber-policies and infrastructure need to be flexible, with the expectation that they will need to be changed when they become out-of-date within the following few years. Adaptability is crucial; if it cannot be changed, updated, or replaced, it has already failed.

As technology becomes integrated more and more into daily life, we will need to change the definitions of existing concepts. Hazelwood and Koon-Magnin (2013) discuss one of the ways our laws have become outdated. In some cases, states have tried to extend legislation involving harassment to cyber harassment by adding to existing legislation. Doing this without

rewriting the definition of harassment itself provides a shaky foundation to build off. We can't think of cyber harassment as an extension of harassment any more than we can consider the front cover of a book the extension of the back; they're still two parts of the same whole. Furthermore, an updated definition of harassment would need to be flexible and able to be redefined every so often to keep up with the rate at which we develop new technology. In today's world, we can't claim to know that what works today will work in the future.

Cybersecurity and Engineering

Engineering is one field that overlaps with cybersecurity, and engineers face challenges because of its variability. According to the National Institute of Standards and Technology (2017), "Systems security engineering provides an elementary approach for building dependable systems" (p. 39) meaning that these engineers are the ones that design and maintain an organization's security system. This is a job that requires constant innovation and coordination with people who hold other roles within the organization for the system they've created to run smoothly. Engineers may use encryption, intrusion detection, and other methods in their design to keep the system secure (Bourgeois, 2014).

Security is always evolving, and so are the best ways of maintaining it, so engineers need to adapt to keep up with the changes, just like the rest of the world. A good way of making sure a system is secure is by building it to be based on security from the start; another word for this is "security-by-design." This design will be built on by other cybersecurity experts, so it's important to have a good basis for the system (van Ommeren, 2014, p. 35-39). From this, it is clear that having a strong foundation is important for a cybersecurity system.

Physical and cyber security are very closely intertwined, as attacks against physical infrastructure can affect the cyber system and vice versa. This is especially true for engineers

who work with electric grids—a type of system that we depend on in our daily lives. A security system will never be completely safe, but engineers can reduce the risk of an electric grid suffering an attack by creating stronger systems that are harder to penetrate. Electric grids are very important to protect because any breach will impact people across a wide area. Any issue with the design of the system will leave holes open for an attack. However. by creating systems that have as few issues as possible, engineers can reduce the effects of breaches on the world (ICF International, 2016, p. 27).

These concepts that engineers depend on are ones that affect us daily. Without cyber technology, electric grids, and the systems to maintain them, we wouldn't have the same level of access to information as we do now. We have grown so used to being able to use smart devices and Google that if those things disappeared, we'd feel lost. At the same time, neither of those two things existed thirty years ago, which shows just how fast technology evolves and how quickly society's understanding of how to use it has changed. Cyber-policy in turn will need to work to keep up with this changing world; our strategies need to adapt to the fact that the world in ten years may be much different than the one we live in today. Gone are the days when "technology" just meant electricity and automobiles.

Cybersecurity and Criminal Justice

Engineering is not the only area that is affected by this change. In today's world, a significant number of crimes are committed through technology (Payne & Hadzhidimova, 2019). Because of this, there is overlap between the two fields of criminal justice and cybercrime. For example, one topic that both study is neutralization theory, which states that criminals justify their behavior to themselves in ways that neutralize the crime, even though they know right from wrong (Payne & Hadzhidimova, 2019).

From this, it is clear that human psychology doesn't change much when using technology as a medium. Humans who commit crimes through technology are human in the same way as those who commit crimes without technology. What *has* changed is how we've adapted our lives and our societies accommodate—which can be seen, for example, in the number of children who are cyberbullied by peers. So many cases of bullying involve technology that instead of seeing cyberbullying as *separate* from regular, in-person bullying, I believe that cyberbullying should be considered a *type* of bullying. Including cyberbullying within the definition of normal bullying would give anti-bullying laws a more comprehensive definition of what bullying means in our world today and help families of bullied children to seek justice.

The fact that many cybercrimes are committed internationally, or in ways that make it hard to catch and prosecute the offender, shows just how globalized technology has made our societies. Technology has given us a way to connect the entire physical world. Because of this change, having a strong system in place that acknowledges a new definition of cybercrime is crucial.

The same is true across all disciplines; when making cyber-policy involving security, we shouldn't see the cybersecurity system as being completely self-contained. Cybersecurity should be considered a type of security that is on the same level as physical security, in the same way that cyberbullying should be one of several types of bullying. In my opinion, the world of technology shouldn't be seen as completely separate from the physical world.

Conclusion

From this, it is clear that flexibility in the way we make cyber-policy is necessary. Technology changes very rapidly, which is a challenge engineers already face in maintaining their systems. Also, viewing the cyber world as an extension of the regular world instead of part

of it means that cyber-policies could end up being left incomplete. Technology doesn't exist in a vacuum; it impacts our lives every day.

Some might argue that it's important to keep disciplines separate and only see cybersecurity as overlapping with other disciplines. It's true that cybersecurity is multidisciplinary and shouldn't be completely broken into separate categories. However, it's not the field and the way it's organized that we need to change; it's the way we see technology in general. The issue is that the cyber world is sometimes separated from the physical world, when they are constantly feeding into each other. Changes in the cyber world have impacts on the physical world and vice-versa, so treating these two as separate only lets us see part of the issue.

Some also might say that it's unnecessary to constantly update definitions to accommodate changes in technology. However, I don't think we need to constantly update policies as much as we need to be *ready* to make changes in our policies. We don't know how or how much the world will change in ten years; all we know is that it likely will change. Because we can't see into the future, what we need to do is to be ready to adapt.

I believe that we need to be able to change our policies along with the world, and to accept that the changes will affect not only technology, but society as a whole. We have already seen that changes in technology affect multiple disciplines as well as our society, two of which are engineering and criminology. However, some believe it's better to keep the two completely separate, because there are too many differences for them to be seen as two parts of the same whole. Another viewpoint that some have is that it's more important to have a strong base than to be ready for change. While I disagree, these are still important topics to consider.

References

Bourgeois, D. (2014). Information Systems for Business and Beyond. Retrieved September 22, 2019, from https://drive.google.com/file/d/1DxwGumLqWmoqjYT0XFekMu6dFg3ev4Eh/view

Hazelwood, D. & Koon-Magnin, S. (2013). Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis. Retrieved December 1, 2019, from http://www.cybercrimejournal.com/hazelwoodkoonmagninijcc2013vol7issue2.pdf

ICF International. (2016). Electric Grid Security and Resilience: Establishing a Baseline for Adversarial Threats. Retrieved September 22, 2019, from https://www.energy.gov/sites/prod/files/2017/01/f34/Electric Grid Security and Resilience--Establishing a Baseline for Adversarial Threats.pdf

National Institute of Standards and Technology (U.S.). (2017). An Introduction to Information Security. Retrieved September 22, 2019, from https://drive.google.com/file/d/1F4UD29y91CF47MvnSKAI1OHmj60YqB3V/view

Payne, B. & Hadzhidimova, L. (2019). Cybersecurity and Criminal Justice: Exploring the Intersections. Retrieved November 10, 2019, from https://drive.google.com/file/d/1AJ5R5Ia7KLp7GK9Ndt6uAF6ESWYQ9HqI/view

van Ommeren, E., Borrett, M., & Kuivenhoven, M. (2014). Staying ahead in the Cyber Security game: What Matters Now. Retrieved September 22, 2019, from https://drive.google.com/file/d/138J6FOI3XLjz87rb0t73v4xoZIcmGp9z/view