Current and Future Policies: Can Cybersecurity Adapt for the Coming Future?

The intersection of cybersecurity and criminal justice, digitized DNA, and attacks on critical infrastructure all contribute perspectives on the effectiveness of current cyber policies and provide insight on how future policies will take shape for future technology

The Intersection of Cybersecurity and Criminal Justice

Definition

Cybersecurity and criminal justice exist as mostly separate fields of study, but the growing technological landscape reveals a need for the integration of the two. Criminals will always find ways to exploit new and evolving technologies, making the idea of cybercrime change and evolve as well.

According to a study done by Payne & Hadzhidimova, in a sample of 365 cybersecurity programs from 615 institutions at the graduate(?) level only 17% of the programs offered courses related to criminal justice. Similarly, in the same sample of institutions, from 531 criminal justice programs, only 16.2% of the programs offered cybersecurity courses (Payne & Hadzhidimova, n.d., p. 9, 11). Despite the growing prevalence of crime in the cyber field, there does not appear to be a push for the combined study of cybersecurity and criminal justice when there could be a benefit to do so.

Examples

Like previously mentioned, criminals will find a way to exploit current technology, which means… The combined study of the two fields could provide insight into things like "...(1)defining cybercrime, (2) explaining cyber offending and victimization; (3) identifying

guardianship activities, (4) measuring victimization and offending, (5) developing future employees, (6) expanding the field of digital forensics, (7) determining interventions, (8) developing, researching, and understanding cyber law, (9) seeking NSA Designation, and (10) conducting interdisciplinary research" (Payne & Hadzhidimova, n.d., p. 2).

Mitigation techniques

It may be difficult to coalesce the two areas since cybersecurity in particular has historically been associated with other STEM fields (Payne & Hadzhidimova, n.d., p. 15). Cybersecurity on its own typically requires technical knowledge related to coding, which may not interest those in criminal justice due to inaccessibility or lack of knowledge. They may also not feel like cybersecurity is related to their field of study. Similarly, those in cybersecurity may not see criminal justice as relevant because of the different skillsets needed. In looking at the types of jobs in cybersecurity, it is possibly clearer how criminal justice can be applicable to the field. Jobs such as cyber insurance policy specialist, cybercrime investigator, and cybersecurity lawyer (Morgan, 2023) all could have influence from criminal justice. Encouraging the adoption of both fields ensures that as the technological landscape expands, there will be experts in the future who can guide new laws and frameworks into place.

Connections

Digital technology will continue to grow in ways that people are not adequately prepared for, and that includes cybercrime. Not too long ago, biometrics as a form of cybersecurity seemed out of reach. Yet, now facial recognition is used to unlock smartphones and fingerprint scanners are used as two-factor authentication. In the near future, it is possible that identifiers such as social security numbers will be done away with in favor of DNA scanning. While this

may offer stronger identification methods, digitizing DNA offers new ways for bad actors to commit crimes, in ways that are not currently anticipated.

This evolution of cybercrime will warrant new discussions and potentially new laws and regulations about digitized biometrics. This could be made easier with already-established interdisciplinary experts.

Digitized DNA

Definition

Official government documentation is used to verify identity. If these items are stolen or compromised, new ones are issued. In the future, it is possible for DNA to replace these documents as DNA is intrinsic to the person it belongs to. However, it may still be possible for identity theft to happen and if it does, there may not be any recourse for the person affected because a person cannot simply get new DNA.

Examples

Like any personal information available, stolen DNA could end up in bad places, such as the dark web for hackers to exploit (Aldbaugh, 2025).

Mitigation Techniques

It will be very difficult to restore damage done due to stolen DNA. Further study will need to be done in order to find solutions to resolve this very unique situation. Studying the issue before it actually becomes reality will prepare all parties involved before the situation arises.

Connections

Identity theft is an already established cybercrime that harms many individuals today. The introduction of digitized DNA as personally identifiable information will further expand the breadth of cyber identity theft. The prosecution and victim recourse of these crimes will need to

be contemplated and evaluated by people who are knowledgeable in all fields involved. There will need to be people who can accurately assess the damage and offer solutions to mitigate the issues

Cyber Attacks on Infrastructure

Definition

Threat actors are now able to extend harm beyond the digital space by finding ways to take down critical infrastructure through attacks on the digital systems. This is able to happen typically because the cybersecurity measures put in place are either breached easily or not utilized at all.

Examples

In 2023 and 2024, threat actors were able to gain access to Industrial Control Systems (ICSs) that serviced water systems, energy systems, and other education and government infrastructures. The attacks resulted in disrupted services for thousands of people across the US (2024). One such attack on a water system in Texas "... tampered with their water pumps and alarms, causing water to run past designated shutoff levels and overfill storage tanks" (2024).

Mitigation techniques

Some of the easiest ways for bad actors to access systems is through default passwords and outdated software. Many of the attacks mentioned above could have been avoided through following NIST guidelines and cyber policies. Simple steps such as changing passwords, keeping system software up-to-date, and managing access control can be very effective at mitigating attack points, but they are often not done because they are not seen as priorities (2024). Stronger regulations and enforcement of cyber policies can ensure that these steps are taken seriously.

Because these attacks target infrastructure, regulations could be put in place to ensure that companies follow cyber policies in order to protect the people.

Connections:

Critical infrastructure includes institutions such as hospitals, which often collect and store sensitive information about patients. In the age of digitized DNA, hospitals will have a greater responsibility in protecting the data of the people they serve. While it is critically important now for hospitals to take cybersecurity seriously, it will only become even more critically important if and when hospitals store the digitized biometric data of their patients. It will be difficult to restore stolen identity via DNA. There should be a large amount of consideration put into what cyber policies should be in place to protect the data.

Discussion:

Current cyber policies, while effective, do not always have the ability to quickly adapt to the changing landscape. Technology will be utilized in ways that experts are not prepared for and policies will need to be adapted quickly to minimize the downtime needed to catch up.

In looking at the attacks on infrastructure, it is apparent that current cyber policies and frameworks are often underutilized, which leaves critical institutions vulnerable. Policies and regulations tend to be more reactive to attacks rather than proactive in protection. Verbeek's "intelligification" (Verbeek, 2014) prediction could be closer than anticipated and it has the potential to create more opportunities for cyber threats to emerge. The current system of reacting to threats as they happen may not be as effective in the future due to the ability for cyber threats to attack areas that they could not before. Recognizing the prevalence of technology and its integration with the human experience will be critical for addressing the new threats. The new experts (such as those who study the integration of cybersecurity and criminal justice) will be in

a unique position to set precedents and guide the policymaking that will affect the technological landscape going forward. These precedents will likely affect the adoption of future technology like digitized DNA.

Conclusion:

Current cyber policies tend to be reactive towards changes in the technological landscape in regards to new threats. While there are ways to mitigate threats before they happen, they are not as effective in reacting to new technologies that emerge and the threats that also emerge as a result. Policies and regulations tend to need to catch up to threats instead of keeping pace or getting ahead of them. With the growing prevalence of technology and new technology emerging very often, it will be important for the policies to keep up. When regulations and enforcement are lacking, situations like the past attacks on infrastructure occur. However, with new experts such as those in criminal justice and cybersecurity, it could be easier to create policies that can adapt to new technologies, like the future digitized DNA. Continued research and development into interdisciplinary fields could be the key to finally keeping pace.

References

Payne, B., & Hadzhidimova, L. (n.d.). READING: cybersecurity and criminal justice: exploring the intersections (payne-hadzidimova). *INPRESS at international journal of criminal justice sciences*.

Morgan, S. (2023, September 24). *50 Cybersecurity Titles That Every Job Seeker Should Know About*. Cybercrime Magazine. https://cybersecurityventures.com/

Aldbaugh, H. (2025). Chapter 4: Biocybersecurity. In *Cybersecurity, Technology & Society* (pp. 55–63). essay.

Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024. (2024, June). *Www.Dni.Gov*. Retrieved from https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf.

Verbeek, P.-P. (2014). Designing the public sphere: Information technologies and the politics of Mediation. *The Onlife Manifesto*, 217–227. https://doi.org/10.1007/978-3-319-04093-6_21

Appendix A

Reasoning Notes

The topics covered in this paper were all of interest to me. Infrastructure attacks encompass some of the challenges that we are facing now with our current cyber policies and digitized biometric data and DNA represent the direction that we will eventually move toward with new challenges. These topics are a look into our current cyber challenges and what they could be in the future. I never could have imagined that a person's DNA could be "stolen" in that capacity and it makes me question how we handle things like data privacy in the future.

I was also interested in intersecting criminal justice and cybersecurity. I have always viewed these fields as separate areas of study solely based on one being STEM-based and the other being law-based. I understand, especially in the context of the changing digital landscape, how important it will be for these two fields to work with each other. It made me think about how the two other topics relate to the intersection as it stands now. If I wanted to change careers in the future, delving into that intersection could be an interesting place to start. The world will need experts like that in the future.

Was AI used in writing this paper? No. While I am not wholly against the usage of AI, I strictly avoid using it in an academic setting. I first attended college from 2014 to 2019 and was able to get through without any AI usage and I continue to do so in order to prevent reliance on it. This paper was entirely written by me (with the help of an APA citation creator and online dictionary/thesaurus).