Danielle Caplinger - December 6, 2024

Bio-Cybersecurity & The Short Arm of Predictive Knowledge

The long-term effects of the increased intelligification of biotechnology will have several important implications for biocybersecurity that must be addressed now.

The Short Arm of Predictive Knowledge

Introduced by Hans Jonas, the idea of a short arm of predictive knowledge encompasses the idea that although an idea, or a new technology, is well-intentioned, there is no way to understand its consequences months, years, or centuries in the future (Jonas, 1973, p. 37). This can be applied to many industries, but I believe it is most prevalent in the intersection between cybersecurity and biotechnology. The world of biology and biotechnology is a vital one; one where technological advancements help improve the health and lives of thousands of people around the world. However, the intelligification of such technologies, especially with little regard to cybersecurity, puts us in the midst of this short arm where we cannot accurately predict the consequences of how biotechnology will create cybersecurity issues in the future.

What is Bio-Cybersecurity?

Bio-cybersecurity, sometimes known as cyber-biosecurity, is the use of cybersecurity practices for biological information and biotechnology. As technology has grown in the last few decades, advancements have been made to integrate such technologies with biological components in order to help those with diseases, genetic conditions, and other health-related concerns. As with any technology, cybersecurity is important to keep this biotechnology secure

from unwanted access, alterations, and other cybersecurity incidents. This becomes especially true as more and more biotechnological devices become “intelligized” or become smart-devices with even more connection and dependency on the internet.

The Scope of Current Bio-Cybersecurity

Current bio-cybersecurity procedures play a key role in confidentiality of private health information, especially in the United States where HIPAA sets standards for how such information is kept private and secure. In the last decade, there was even an addition to HIPAA standards to add genetic information to the list of protected private health information (PHI). There is also an increase in moving security solutions to a cloud-based environment, albeit a slow movement, that outsources security from the health institutions and biotechnology manufacturers to cloud-based SaaS providers (Whelan, 2022). Other cybersecurity standards including encryption, multi factor authentication, firewalls, IDS, and network monitoring are also standards in today’s world of bio-cybersecurity. However, the healthcare industry, and by extension biotechnology, is the most targeted industry in the world by malicious cyber actors (Whelan, 2022). As more and more of this industry integrates with technology, this threat will only grow.

Possible New Developments

Although it would be impossible to predict the exact way that technology will advance in the next several years, I believe that a few types of technology will be developed and implemented during that time frame. For starters, long-term devices like pacemakers and insulin pumps will become connected to the internet for both patient and doctor monitoring. There are already some

primitive versions of this to help reduce the time that patients spend in-office for long-term care. I predict that these types of medical devices will continue to become "Smart" devices to increase this type of efficiency. Additionally, gene editing technology, already in its early stages with CRISPR, will continue to advance to the point where more diseases are combated at the genetic level. My final prediction regarding bio-cybersecurity is the use of biometric technology to create synthetic organs through 3D printing and gene formatting. This type of technology would revolutionize the organ-donation industry and allow for more individuals to get the life-saving care that they need, and often have to wait years for.

Long-Term Concerns

All of these technologies will create amazing health benefits for patients around the globe, but there are many long-term concerns that I don't believe have been adequately addressed. [1] For starters, devices like pacemakers and insulin pumps must use specialized software that will be increasingly difficult to secure. Additionally, implantable devices would be almost impossible to access quickly in case someone needs to physically access the device for security updates. There are also long-term concerns when it comes to the advancement of gene editing. This technology is only as good as the software and devices that run it, meaning if malware were to be used against such technology, the genes could be damaged beyond repair. [2] Additionally, there is a possibility that a malicious attacker could create an entirely new type of cyber attack in the form of DNA malware, as evidenced by a research team at the University of Washington (Coldeway, 2017). Finally there are concerns regarding 3D printed organs because protecting this type of information from IP threats would be incredibly hard since healthcare IP is one of the most sought-after data types existing today.

Implications (Why is it a concern?)

All of these technologies have long-term concerns that must be addressed, but to do so appropriately, we must first understand why these are such important ideas. For starters, the security of devices like pacemakers is of the utmost importance because they interact with the lives of normal people. If a hacker were to gain access to someone's pacemaker due to poor security controls, they could potentially kill that individual. [3] In this future of bio-cybersecurity, it is not just data at stake, but human lives. Similarly, the future of gene editing could lead to a malicious actor using this software to not just create computer viruses, but biological viruses that could infect and/or kill thousands of people. Finally, the implication of digitizing human organs to any extent using 3D printing creates the possibility of integrating them with computing capabilities for monitoring. [4] If this were to happen, the entire human body could become a new attack surface for malicious hackers to take advantage of.

Possible Solutions

Although all of these technologies have the potential for great harm, the role of cybersecurity stays the same: to secure these biotechnology systems and mitigate this harmful potential to the best of its ability. For starters, all of these technologies must be developed with a security mindset from design all the way to implementation. This will keep them from falling into the same problems that we currently face with aged critical infrastructure that was designed without security in mind. We must also make all of this PHI, Intellectual Property, and connections to these devices encrypted with the highest standards available at the time, with the possibility of upgrading it as necessary. This idea must also be integrated into security standards that are created regarding how these technologies are kept secure as well as ways of adapting security as

new technologies emerge. Although I believe that all of these solutions must be implemented, none of these will offer 100% security. That is a price that we must accept if we continue to advance biotechnology, and one that must be mitigated to the best of our ability by cybersecurity professionals.

Conclusion

Bio-cybersecurity is an emerging field that is almost impossible to accurately predict with any accuracy. That being said, we can take our knowledge of other evolutions in technology to hazard a guess about what the world of bio-cybersecurity could lead to. Nevertheless, the key to addressing these issues lies in preparing ourselves, and our cybersecurity policies, now to not be left behind as technologies evolve at an unprecedented rate. Just as biology and technology will converge even further in the future, so must cybersecurity and such technologies.

References

Coldeway, Devin. (2017). Malicious code written into DNA infects the computer that reads it *TechCrunch.* https://techcrunch.com/2017/08/09/malicious-code-written-into-dna-infects-the-computer-that-reads-it/

JONAS, Hans. (1973). TECHNOLOGY AND RESPONSIBILITY: REFLECTIONS ON THE NEW TASKS OF ETHICS. *Social Research*, *40*(1), 31–54. http://www.jstor.org/stable/40970125

Whelan, Sarah. (2022). Tackling Cybersecurity Threats in the Biotechnology Industry. *Technology Networks Informatics.* https://www.technologynetworks.com/informatics/blog/tackling-cybersecurity-threats-in-the-biotechnology-industry-364979