Deandre Turner

Old Dominion University

CYSE 200T: Cybersecurity, Technology, and Society

Professor Chris Bowman

June 3, 2025

Cyberbiosecurity: Protecting Biological Data in the Age of Digital Threats

BLUF

Technologies innovative constantly nowadays. People personal data are always at a state of vulnerability if not handled properly. This could include DNA, medical records, and even biometrics. Cyberbiosecurity is a growing concern on a national level and should be looked upon with great interest.

The Increasing Case of Cyberbiosecurity

As technology advances, our day-to-day lives become more and more digitalized. This includes our very biological components. In the article *"Hacking Humans: Protecting Our DNA From Cybercriminals,"* it discusses what is called "cyberbiosecurity". It is described as "the slew of risks that can come with the increase in digitization in life sciences" (Rizkallah, 2018, para. 3). Digitalized DNA plays a bigger and more important role than what it seems. We should be enveloped in creating forms of protection pertaining to our biological and biomedical data. As people begin to invest in technological endeavors such as DNA testing and health technologies, this leaves people vulnerable to data extractors. Unlike something like a password or a Social

Security number, once compromised, the effect is far more devastating than traditional identity theft (Rizkallah, 2018).

Targeted Health Care

One industry that is impacted the most is the healthcare system. According to the Council on Strategic Risks (2023), "healthcare cyber threats account for 24.5% of all hacks, with each breach costing an average of $5 million" (para. 6). Hackers can use data from these institutes to take advantage of victims. Biological data can be manipulated or even weaponized. They could, for example, use malware in systems like HVAC and shut down a medical center while also extracting data. Hackers could hack using DNA malware, sabotaging machines that analyze an individual's health. Other instances could consist of malware in synthetic DNA, leaks from containment laboratories, or even extracting data to build bioweapons such as pathogens. This also includes cases in which certain supply chains are halted due to cyberattacks. As technologies advance and hacking becomes more sophisticated, this leaves data like this very vulnerable (Murch et al., 2018).

The Response and Protocol

As such, when tackling this issue, multiple personnel should play a factor in the grand scheme of things. We are going to need cybersecurity experts, biotechnologists, and policymakers. To avoid this, lawmakers need to implement certain policies and procedures to prevent such occurrences. An example of this could be creating policies that make it mandatory to educate facilities to prevent this. People are prone to just apply to 23andMe, not knowing the details about their genetic information (Rizkallah, 2018). Biotechnology needs to have certain protocols such as backing up data, which might include physical official copies of digitalized

information. Cybersecurity needs to create systems that prevent hackers from gaining access to data in the first place. This could be in the form of software or even authentication and authorization confirmations. Certain questions might arise from this, such as: should employers ask and screen an individual's genetic information? What about if the government has access to this data, should they be allowed to use it?

Conclusion and Preparation of Cyberbiosecurity

To conclude, cyberbiosecurity is a national issue that must be addressed and handled with proper care. This issue is becoming increasingly more complex and difficult to understand. The best thing we can do is start finding solutions and protocols to protect people from this extortion. We could start using more firewalls, better regulations, and even education to make people aware of these issues. When institutions begin to co-opt for collaboration, they innovate and fight against this issue. We must do everything in our power to stop this vulnerable issue.

Reference:

1. Council on Strategic Risks. (2023, September 14). *The cyber-biosecurity nexus: Key risks and recommendations for the United States*. https://councilonstrategicrisks.org/2023/09/14/the-cyber-biosecurity-nexus-key-risks-and-recommendations-for-the-united-states/

2. Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy. *Frontiers in Bioengineering and Biotechnology, 6*, 39. https://doi.org/10.3389/fbioe.2018.00039

3. Rizkallah, J. (2018, October 1). *Hacking humans: Protecting our DNA from cybercriminals*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2018/10/01/hacking-humans-protecting-our-dna-from-cybercriminals/