Elizabeth Howard

CYSE 200T

4/28/25

Analytical Paper

Where Biological Science and Cybersecurity Interrelate: Ethical Considerations in Gene Editing

Gene editing presents serious ethical risks if not carefully regulated, particularly as advances in biological science technology accelerates and with it the vulnerabilities in cyber-infrastructure increase. One major issue we explored in the field of biological sciences is the handling of genetic information and its potential misuse. In alignment with the principle of proactively considering the long-term consequences of technological development, I propose that policymakers should prioritize removing sensitive genetic records from online systems. Instead, a secure infrastructure should be developed where genetic information is transferred and stored exclusively in physical (paper) formats to mitigate cyber threats and protect against long-term societal harm.

Unethical Practices and Future Potential

I believe that gene editing could be unethical if managed improperly. As advances in biological science and gene editing accelerate, the development of robust cyber-policy and infrastructure must expect not only immediate security risks but also the profound long-term societal impacts these technologies may unleash. According to the Innovative Genomics

Institute, determining the ethics of gene editing "…involves weighing competing factors that often cannot be easily measured, for example the risks or benefits of action or inaction in the long-run, or whether permitting a broadly acceptable use of a technology might open the door to other uses that would be more controversial." (Henderson and Halpern, 2024). This shows that there is much to learn about its effects on our future. Including the possibilities of cyber-attacks that can jeopardize its safety. Which leads me to my next topic, the possible hacking of DNA fragments.

Malware and DNA

According to *Cyberbiosecurity: Advancements in DNA-based information security* (Tuoyu et. al., 2024) "Malicious codes intended to attack computer systems can be stored as artificially synthesized DNA fragments, which can be released during DNA sequencing and decoding and attack computer and network systems." I propose that in the future as technology increases and vulnerabilities incline due to positive correlation policy makers will need to address the necessity to take these records offline, creating an infrastructure where genetic information is only transferred and stored in paper form. This will completely avoid the possibilities of cyber offenders misusing this data. Which leads me to my next topic, the potential for individuals to become targets.

Human and Hacking and Individuals as Targets

Personal genetic information is very vulnerable and valuable data. As we continue to digitize of our lives, the future holds the potential for large genetic databases to be easily accessible to gene-hacking (Simana, S., unk.). According to Hacking Humans: Protecting Our DNA From Cybercriminals, "Hacking humans will continue… The addition of DNA as a new

avenue for hackers to explore is yet another new frontier that cybersecurity professionals need to dace head -on." (Rizkallah, J. 2018). Any time we are discussing changing the way natural things are made there could be an issue because you are trying to take the power of creation into your hands without knowledge. In this case it is the knowledge of how to protect individuals that we do not fully possess. Now let's look at medical inequality in relation to cybersecurity.

Social Inequality and "Cyberbiosecurity"

Gene editing technologies, particularly therapies, are generally extremely expensive, often costing millions of dollars per treatment. According to *The Health Equity Implications and Role of Community in Gene-Editing Research and Applications* "Far from being a theoretical concern, many non-CRISPR gene therapies cost between $450 000 to $2 million per treatment with the gene therapies Hemgenix and Zolgensma costing $3.5 million and $2.1 million, respectively, per 1-time treatment." (Subica, AM., 2023). "These extraordinary costs place gene therapies primarily within the reach of society's most advantaged while excluding much of the population." (Subica, AM., 2023) This could lead to medical inequality. In addition to that those who are underserved or are poverty-stricken may not be able to afford the necessary protections of keeping their genetic data safe.

Arguments

While I agree that scientific knowledge is meant to be openly shared so that the scientific community can build upon it. Many would argue that taking the continuous gene editing research offline would slow down progress and limit the benefits of gene editing. However, when it comes to altering the creation of life we must exercise extreme caution. The potential dangers brought about by the cybersecurity vulnerabilities of these advancements is not worth the risk. It

could lead to gene mutations and loss of life down the line. We must consider the long-term results of gene editing technologies for years to come.

Political and Scientific Effects on the Individual

It could create and may already create even greater rifts in the political and scientific communities when it comes to regulation of the gene editing process. According to *The Ethics and Security Challenge of Gene Editing*, "gene-editing decisions should be left to individual choice" (Biberman, Y., 2023). That is honorable if it is sustainable. However, when we look at our political climate, we see the potential for anything to be manipulated for personal gain. They may say the choice is up to the individual, but how long until that right is taken away? How long until they begin to omit consent and personal choice in the name of "science"? History proves this possibility with the case of such as Henrietta Lacks and the use of her cancer cells or the Nazi experiments. How much more can this type of exploitation exist with advanced technology?

Conclusion

Overall, my analysis concludes that the only true way to avoid the unethical misuse of data from gene editing is to remove it from the reach of cyber criminals by taking it offline. We see this need based on the evidence that future factors cannot yet be measured, DNA fragments could be sequenced with malicious codes, and it can lead to medical and information security inequality. While there are major trade-offs to consider the priority is to secure the long-term safety of genetic information instead of settling for short-term convenience. Even though some may argue that scientific knowledge should remain online to be built upon and learned from. It is too great of a risk. In the future it will be necessary for determination that certain gene editing

data be removed from the cyber world and transferred and stored by an alternative physical means.

References:

Henderson HR, Ramit G, Tolpa T, Murdock AG, and Halpern J. (2024) CRISPR & Ethics. In Hochstrasser et al. (Eds.) CRISPRpedia. Innovative Genomics Institute, University of California, Berkeley. Retrieved from: https://innovativegenomics.org/crisprpedia/crispr-ethics/ (Last updated: November 21, 2024.) https://doi.org/10.60640/G2H59Q

Simana, S. (unk.) The (Possible) "Dark Side" of Gene Editing Technologies. The Petrie-Flom Center. Par. 6, https://petrieflom.law.harvard.edu/2019/12/10/the-possible-dark-side-of-gene-editing-technologies/#:~:text=The%20Potential%20to%20Target%20Individuals,using%20it%20for%20illegitimate%20purposes.

Subica AM. CRISPR in Public Health: The Health Equity Implications and Role of Community in Gene-Editing Research and Applications. Am J Public Health. 2023 Aug;113(8):874-882. doi: 10.2105/AJPH.2023.307315. Epub 2023 May 18. PMID: 37200601; PMCID: PMC10323846.

Tuoyu Liu, Sijie Zhou, Tao Wang, Yue Teng, Cyberbiosecurity: Advancements in DNA-based information security, Biosafety and Health, Volume 6, Issue 4, 2024, Pages 251-256, ISSN 2590-0536, https://doi.org/10.1016/j.bsheal.2024.06.002.