# BioCybersecurity: Ethical Considerations of CRISPR Gene Editing

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 200T: Cybersecurity, Technology, and Society, Professor Chris Brown

February 22, 2025

Assignment:

Based on the following readings related to the BioCybersecurity section of this course, **identify possible ethical considerations** and explain your position.

Sources:

*Malicious code written into DNA infects the computer that reads it*

*Protecting Our DNA from Cybercriminals*

The researchers discovered basic vulnerabilities and attack vectors in the open-source code of the "security infrastructure around DNA transcription and analysis," making them appear inadequate for professional lab research worldwide (Coldewey, 2017). The researchers discovered they could use human DNA, the human genome, to hide, encrypt, unpack, and execute malicious code into a computer. In the transcription application, the researchers sort/comb through the human DNA or raw data for patterns, then transcribe that information into baseline sequential binary code. Thus, the DNA converts into a binary language for a computer to receive, unpack, and understand.

In the study, using the vulnerable transcription application, researchers housed malicious code inside the binary form of the complex human DNA to infect a computer. The researchers would then use dangerous code in a reasonable maximum size to conduct a basic buffer overflow attack: the program writes more data into a buffer (a temporary storage area) than it is designed to hold, and the excess data can overwrite adjacent memory, potentially leading to system crashes, data corruption, or even arbitrary code execution by an attacker (Fortinet, 2025). It operates like a Denial of Service (DoS) and Privilege Execution attacks. In other words, the researchers used human DNA as a pseudo 'Trojan Horse' to house a typical virus, ransomware, and other malware to infect experimental computers.

As the reader, you may be asking yourself, "How does this apply to me? Why do I need to know about this 'existential' threat?" First, the medical storage facilities and organizations become greater attack vectors if they do not have the protocol to detect and prevent malicious code like stealthy buffer attacks that can hide within the DNA digital records. Second, suppose the malicious code found in our DNA uploads and saves to servers and online accounts, and we, the consumer, were to access those records via an internet browser and download the data. In that case, our network and systems can fall victim to the attack.

Lastly, the biggest concern is that the malicious binary code hidden within our DNA infects nearby computers within a wireless range, or what is worse, we become vulnerable attack vectors and become infected with other malicious code that devastates our human genome like a common cold or COVID virus. Essentially, we can turn into walking 'logic bombs' or 'zombie botnets' able to infect any living person or technological device within a specific radius of us. That process can occur vice versa too. The biotechnological transfer between humans and computers and between computers and humans seems crazy and farfetched today. However, those crazy ideas may become

scary realities soon, like in many Science Fiction movies that include gene editing and human cloning in *Blade Runner (1982, 2049), The Island (2005)*, the *Resident Evil Series (2002 – Present)*, and the *Alien franchise (1979 — Present)*. With technological innovations on the rise and the widespread increase in storing DNA data, we will become more vulnerable to higher-level cybersecurity attacks, questioning if the living world is genuinely secure from the virtual world.

## References

Chin, K. (2024, December 24). *Biggest Data Breaches in US History (Updated 2025)*. Retrieved from UpGuard: https://www.upguard.com/blog/biggest-data-breaches-us

Coldewey, D. (2017, August 9). *Malicious code written into DNA infects the computer that reads it*. Retrieved from TechCrunch: https://techcrunch.com/2017/08/09/malicious-code-written-into-dna-infects-the-computer-that-reads-it/

Fortinet. (2025, February 18). *Buffer Overflow*. Retrieved from Fortinet: https://www.fortinet.com/resources/cyberglossary/buffer-overflow

Rizkallah, J. (2018, November 2019). *Hacking Humans: Protecting Our DNA From Cybercriminals*. Retrieved from Forbes: https://www.forbes.com/councils/forbestechcouncil/2018/11/29/hacking-humans-protecting-our-dna-from-cybercriminals/

Wikipedia. (2025, February 16). *History of the Internet*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/History_of_the_Internet