Is DNA Digitalization Worth Continuing?

Kevin A. Loarca

Old Dominion University

CYSE 200T: Cybersecurity, Technology & Society

Professor Christopher Bowman

June 28, 2026

Is DNA Digitalization Worth Continuing?

The integration of human DNA and technology can introduce issues that may not appear as an immediate effect. The topic in question introduces potential risks, which include security and privacy concerns surrounding the combination. Through the philosophical lens of the short arm of predictive knowledge, there is a limited ability to understand the long-term impact this technology will have on society. These issues, however, should not discourage those in the field from pursuing it. Instead, they need to be aware of the potential risks that may contradict the benefits they are trying to achieve. There are remedies to address these concerns, such as recommending cyber policies and restrictive data sharing. Understanding the risks beforehand would allow for potential solutions to the long-term implications that the combination will have in society.

There will always be a security risk when it comes to the use of technology. Even with the best security measures in place, there is no guarantee of preventing a breach of systems. With this in mind, DNA digitization should continue as it provides personal and medical benefits that outweigh the lifelong security risks. As stated in the article, the digitization of human DNA, for the purpose of science and medical research, could bear great fruit in curing fatal illnesses (Rizkallah, 2018). This perspective on DNA digitization is worth the potential security risks, as it benefits society. However, the security risk should not be completely ignored when technology is used alongside these types of scientific advancements. As biological data becomes digitized, there is an important need to invest in security. The presence of permanent biological data changes the view on “human factor” security compared to traditional digital passwords. There is no way to change the biological material, so if there is a possibility of a breach, the information is stolen permanently. Additionally, if the systems were to have the best security, the risk is

present from the people themselves. There are social engineering tactics that malicious actors can use to try to compromise those systems. This becomes far more dangerous if those within the organization are not taught the necessary security practices to prevent that type of attack. Privacy is also another concern that may create hesitancy in continuing this type of research. Without drawing a line on what is considered oversharing, it will create issues. That is why a clear indication is needed to prevent data from being accessed by unrelated parties. The party will use the information for purposes other than what was intended. Additionally, there is uncertainty about how secure their protocols are when it comes to storing information on their systems. If their security protocols are not enough, it will lead to data breaches.

Security Concerns

[1] There is a technical risk associated with the use of DNA digitization. In the article provided by Devin Coldewey, researchers discovered an exploit that successfully infected a computer with a malicious program coded into a strand of DNA (Coldewey, 2017). In the article, the analysis program reads the DNA strand bases and turns them into binary code. The conversion is done using ASCII As, Ts, Gs, and Cs, in which a stream of bits is done in a fixed-size buffer that is assumed to have a maximum read length. This would then lead to a basic buffer overflow attack, in which the program would execute arbitrary code because it falls outside expected parameters (Coldewey, 2017). This attack reveals ethical and security implications present as the technology continues to improve, which have led to biological data being suspicious. As presented in the article, exploits can be performed with the data of the DNA when translated to binary. This would allow the analysis program to be exploited. This example reveals the implications, as now scientists need to be cautious, as there is a possibility that the data may hide harmful code. If there were to be scientific advancements that utilize technology,

they need to be aware of the security risks and have security protocols in place to protect their data and systems.

Additionally, there are other tactics to obtain these systems that involve manipulating a victim into giving confidential information to a malicious actor, which is known as social engineering. Cybercriminals will communicate with the victim by either saying they're from a trusted organization or by impersonating a familiar person to trick the victim ("What Is Social Engineering in Cybersecurity?," n.d.). As time passes, social engineering attacks will increasingly become sophisticated. Fake websites or emails will look realistic enough to trick victims into revealing information. This can be used for identity theft, which is a common way for attackers to breach an organization's initial defenses to cause disruption and harm ("What Is Social Engineering in Cybersecurity?," n.d.). This could happen to anyone, which can also include the organization that is conducting the research.

Possible Solutions to Security Issues.

[2] At the very end of the article, the researchers recommend performing isolation strategies such as using a virtual machine. I believe this would help mitigate this type of exploit, as the resources would be done on a virtual computer. If they were to find a malicious exploit within the DNA strand that could perform these attacks, it would only compromise the VM. They could then just delete the VM and avoid it spreading through their entire network. As for social engineering attacks, the best opportunity to mitigate this risk is through awareness training. Training will teach individuals to defend against these attacks and understand the security culture within their organization ("What Is Social Engineering in Cybersecurity?," n.d.).

Privacy Concerns

[3] The organizations conducting these scientific advancements need to protect information and avoid instances that could violate privacy. Otherwise, it could lead to misuses beyond their original intent, such as the example Rizkallah provides. The author questions where the line is drawn on what is considered oversharing. It should be advised that these organizations be cautious about sharing this information. Access to these databases by unauthorized parties could lead to issues of genetic discrimination in the workplace. For example, an employer could review the genetic makeup of two interviewees and select the one who doesn't pose future health problems that would affect their ability to work. The employer would discriminate against the other person as they create this negative assumption about their health. Another issue arises regarding privacy if these organizations were to share this genetic data with other third-party vendors. There is a risk present, as there is no control for the original sender on how the third party handles the data (Nail, 2025). Then there is uncertainty of how mature or standardized their data programs are, which may not meet the company's needs. Even if the original organization were to have secured data storage measures, it may not be the same with the party they share it with. This would hold severe consequences if that third party were to have a data breach.

Possible Solutions to Privacy

[4] The organizations conducting this research should not share this genetic information with just anyone. If the organization is conducting this research for medical purposes, it should only be shared with similar groups, such as hospitals. Sending this genetic information to unrelated groups, like an employer, will create issues of genetic discrimination. I advise only sharing this genetic information with selective groups like hospitals, as they are required to follow strict privacy laws. For example, HIPAA would require hospitals to establish a national set of security standards to protect certain health information that is stored or transmitted in electronic form (U.S. Department of Health and Human Services, n.d.). Otherwise, if they were to fail, it would be assumed that they would face harsh fines or punishments. This will encourage them to protect the information or end up facing severe consequences.

Conclusion

Throughout the paper, there were instances where there could be impacts that could affect society if DNA digitization were continued without considering the risks. This, however, should not discourage researchers from pursuing the combination as it has beneficial impacts on society, such as medical research and curing illnesses. Instead, they should try to understand the possible risks that could create hesitation and provide solutions to resolve these risks. There were issues with security concerns. These included a new way of exploiting code through a DNA strand and the issue of social engineering that could affect the researchers. Solutions to address the issues included implementing security protocols, such as using a virtual machine and awareness training. Then there is also the privacy concern, which consists of oversharing issues and possible data breaches from third parties. To address these issues, researchers should refrain from sharing genetic data with third parties. Instead, they should only share genetic data if it’s

with similar organizations, such as hospitals, as they follow strict privacy laws. Overall, it is best not to ignore these issues, as it will lead to unintended consequences.

References

Coldewey, D. (2017, August 10). Malicious Code Written into DNA infects the computer that reads it. Perusall. https://app.perusall.com/courses/202530_cyse200t_33004-cybersecurity-technol-society/malicious-code-written-into-dna-infects-the-computer-that-reads-it-_-techcrunch?assignmentId=gnP5LJryhk2eCa556&part=1&filter=all

Nail. (2025, March 6). Third-party data sharing. DataSunrise. https://www.datasunrise.com/knowledge-center/third-party-data-sharing/

Rizkallah, J. (2018, November 29). Hacking Humans: Protecting Our DNA From Cybercriminals. Perusall. https://app.perusall.com/courses/202530_cyse200t_33004-cybersecurity-technol-society/hacking-humans_-protecting-our-dna-from-cybercriminals?assignmentId=2hiDxZ3Qp66dMSHJe&part=1&filter=all&panel=assignmentInformation

U.S. Department of Health and Human Services. (n.d.). Summary of the HIPAA Security Rule. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

What Is Social Engineering in Cybersecurity? (n.d.). Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-social-engineering.html