Synthetic biology and future crime

This briefing identifies eight potential crimes enabled by synthetic biology and suggests some preventative measures to address them.

Summary

Synthetic biology involves redesigning organisms for useful purposes by engineering them to possess new capabilities. This briefing identifies examples of potential crimes that are or could be enabled by synthetic biology, including cyber-biocrime, and suggests some steps that could be taken to prevent them. For example, the introduction of a National Centre for Biosecurity and Biosafety and a continuous "red-teaming"* approach to emerging technology. A full description of the crimes is available in the systematic review.[1]

Cyberbiosecurity addresses the evolving threat of biotechnology misuse and the emerging risks between cyberspace and biology to develop policies to manage them.[2] In addition to traditional cyber-attacks such as exploitation in unsecured networks and manipulated biological data, cyber-biocrime exploits physical processing involving biological materials that could result in unwanted or dangerous biological outcomes.[3]

Introduction

Researchers and companies around the world are harnessing synthetic biology to solve problems in medicine, manufacturing and agriculture. While the use of synthetic biology was previously limited to research institutions, the technology is now widely available, and at decreasing cost: sequencing the human genome in the 2000s, for example, cost $100 million and required highly specialized institutions and expertise.[4] Today this can be done for less than $1000.[5]

Increasing efficiencies in new technology is at the heart of many current transformative research efforts in synthetic biology, but this comes with new opportunities for crime. For example, fully automated and internet-connected laboratories can create opportunities for data exploitation across geographic boundaries, but also the manipulation and misuse of biological material. Internet-connected laboratories could also be used to bypass regulations of a country to conduct experiments in a country which would allow these. The UK Government has acknowledged the difficulty of regulating uncontrolled experimentation of synthetic biology, citing opportunities for criminals to develop new drugs as examples of such risks.[6] Moreover, the ability to design and synthesize custom DNA sequences through DNA synthesis is facilitated by software, digital tools and an increasing amount of genetic data held on databases.

Crime prevention and detection strategies must keep pace with an ever-evolving technological landscape. This will require multidisciplinary expertise involving collaborations between life scientists and computer scientists, bioinformaticians, molecular biologists, and information technologists.[7,8]

An understanding of how advances in synthetic biology could be exploited for crime is essential for policy actors, law enforcement agencies and technology developers alike, as forecasting future crime opportunities enables preventative steps to be put in place ahead of time.

Methods

- **A systematic review of the literature** of current crimes that could be facilitated by synthetic biology as well as predicted trends. The manufacture of biological weapons** or medical devices is not included here as there is already an established body of work on security concerns in these domains.
- **Interviews** with representatives from academia, the biotechnology sector, UK National Security experts, and "biohackers."*** Experts were asked to identify future crime trends facilitated by bio-technology, and what (if anything) they think should be done to safeguard against them.

Current and future crime risks

This briefing includes eight examples of crimes enabled by synthetic biology. A full description of the crimes is available in the systematic review.[1] These are divided into current crime risks which could occur now, or have already and future crime risks, which are either speculated, or already demonstrated to be possible in the next five or more years.

Crime is traditionally defined as illegitimate activities that are punishable by law. However, this research includes emerging crimes, or those that have not yet taken place. Assessing these with current legislative frameworks may not take into account future evaluations that may categorise certain technologies and their applications as "private matters/decisions". An example of this would be genetic engineering for cosmetic applications. Therefore, "crime" is used interchangeably with the term "misuse" to include both currently illegitimate activities punishable by law, as well as the exploitation of legitimate activities for alternative/immoral purposes.

Current crime risks

Bio-discrimination:

The use of biological data to discriminate against different categories of people on the grounds of their biological information. This could be anything from genomic data (DNA) to any (personal or health related) data. The increased availability and accessibility of biological data on such databases has led to privacy concerns such as the potential for leaked information on genomic data. For example, it could enable bio-discrimination by health insurers who infer information about an individual (such as their ancestry) when calculating their disease risk. It could also enable attacks targeted at high-profile victims where their health/disease data are sold and extorted for ransom.

Cyber-biocrime:

A new type of crime is created as digital and biological systems increasingly intersect via internet-connected laboratories and equipment. There have already been instances of systems being targeted by criminals with inadequate security during the COVID-19 pandemic. For example, hackers from Hostile states reportedly targeted British universities to steal research on vaccine production.[9]

Bio-malware:

Criminals could obtain information by gaining remote access to a competitor's computer system through biological malware – a physical DNA sample containing malware, designed to gain remote access to the computer analysing DNA samples. While this was an orchestrated attack by researchers as a proof-of-concept, criminals could attempt to replicate this attack for nefarious purposes, or find similar vulnerabilities to exploit.

Nefarious biohacking:

The rapidly declining costs of tools for gene editing has enabled people to practice "biohacking".*** For example, an enterprise run by a biohacker selling genetic engineering kits for "at-home" experiments. The commercial uptake of biohacking has led to an evolution of companies willing to provide drugs and/or supplements tailored to the customer's genetic makeup (for example, obtained through saliva samples) for cognitive enhancement. While bio-hacking has the potential to materialise personalised medicine and is being pursued for beneficial purposes, this trend could lead to illegal/unregulated drug manufacturing. Users may begin to produce desired active ingredients that may not be produced naturally, introducing "Do-It-Yourself" drugs.[10]

Future crime risks

At-home illicit drug manufacturing:

Motivated by the emerging commercial uptake of "biohacking as-a-service," criminals could use gene-editing technologies to create new psychoactive substances, manufacture illegal drugs or manufacture counterfeit drugs. Since this process involves the production of desired substances using fast-growing genetically modified microorganisms, such as bacteria in a petri-dish, and does not require cultivation of fields of plants, it has the potential to disrupt and decentralise drug trafficking and offer new opportunities for criminals.

Illegal gene editing:

Black markets providing unapproved and unregulated genetic enhancements such as designer babies could emerge. In 2016, a simi-lar pattern was seen in U.S. stem cell clinics, where 570 clinics were found to offer unapproved treatments for medical conditions and for cosmetic enhancement which were unaffordable via public healthcare.[11]

Genetic blackmail:

A low-probability, but high-impact scenario in which an individual would misuse DNA information for extortion. Examples might include using fabricated (synthetic) DNA to threaten paternity suits against high profile individuals, or using an individual's actual DNA to exploit them financially by claiming that they are related, for example. Biological data could be obtained through hacking of commercial databases (such as those of companies that offer home DNA testing kits), by "DNA-phishing" (obtaining DNA or other biometric data secretly in order to analyse or manipulate) or simple theft of discarded physical DNA samples.

Neuro-hacking:

Supplements available in the wellness market contain bacteria that are engineered to induce a "healthy" balance of the gut when consumed. For example, probiotics and prebiotics that can relieve digestive symptoms by improving or restoring gut health. A growing body of evidence suggests that the gut can impact on the brain (and vice versa), including influencing behaviour and mood.

This interaction could be exploited for malicious purposes in the future in the form of "neuro-hacking". For example, new supplements that leverage genome editing tools could be sold to individuals that impact their brain negatively such as altering mood or impinging on their productivity – via their gut. Individuals could be covertly targeted with these "gut-therapies" without the perpetrator being detected. There is also a potential fraud angle, whereby a scammer claims a person requires a medical product using gene editing techniques, then provides the victim with a fake product or placebo.

Preventative measures to address cyber-biocrime

Current measures intended to combat biotechnology misuse are limited to the use of biological agents in isolation and do not fully consider vulnerabilities in today's lengthy supply chains. Today, biotechnology comprises integrated workflows that increasingly depend on computer-controlled and automated systems. This creates efficiencies but also new opportunities for biotechnology misuse.

Forecasting future crime opportunities that may be facilitated by emerging technologies,

such as synthetic biology, enables preventative steps to be put in place ahead of time to safeguard against potential misuse. A geographically and culturally diverse group of stakeholders involved in this study agreed that cyber-biocrime is highly likely in the form of breaches and for corporate espionage and that cyber-biocrime will first take place where cutting-edge technology is being pioneered, such as within academia.

Stakeholders suggested that the mitigation responsibility for preventative measures to biotechnology-facilitated crime rests with national governments. In addition to creating cyber-biosecurity policy and standards, a national governing body was suggested to be a way to proactively (and if that fails, reactively) reduce the cyber-biosecurity associated risks to human health, including from pandemics. This would provide a clear mandate, dedicated resources and focus to the cause. For example, a National Centre for Biosecurity and Biosafety could assess integrated systems of biotechnology to apply controls of security, through supply chain tracking and management systems, licenses and registrations of purchased supplies. This could strengthen preparedness whilst driving a positive change in culture towards improved "cyber-bio-hygiene".

Shaping of cyber-biosecurity policy

The research team have now proposed the Hybrid Hackathon Delphi Model as a crime prevention methodology and security enabler.[12] This is a "red-teaming" approach to be used as a framework for assessing emerging technologies for their potential for misuse as they are being developed. It captures current and nuanced opinions of diverse field experts while also generating detailed hacking proposals that can be used to aid national security decision making.

References

1. Elgabry, M., *et al.,* 2020. A Systematic Review of the Criminogenic Potential of Synthetic Biology and Routes to Future Crime Prevention. Frontiers in bioengineering and biotechnology, 8, p.1119.
2. Peccoud, J., *et al.,* 2018. Cyberbiosecurity: from naive trust to risk awareness. Trends Biotechnol. 36, 4–7. doi: 10.1016/j.tibtech.2017.10.012
3. Mueller, S., 2021. Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future? Biosafety and Health, 3(1), p.11-21.
4. NHGRI. The cost of sequencing a human genome. Available at: https://www.genome.gov/about-genomics/fact-sheets/Sequencing-Human-Genome-cost
5. The rate at which DNA sequencing costs decreased out paces Moore's Law https://www.genome.gov/about-genomics/fact-sheets/DNA-Sequencing-Costs-Data
6. UK Government, 2019. Future Technology Trends in Security. Available at: https://www.gov.uk/government/publications/future-technology-trends-in-security
7. Murch, R. S., *et al.,* 2018. Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy. Front. Bioeng. Biotechnol. 6:39. doi: 10.3389/fbioe.2018.00039
8. Richardson, L. C., *et al.,* 2019. Cyberbiosecurity: a call for cooperation in a new threat landscape. Front. Bioeng. Biotechnol. 7:99. doi: 10.3389/fbioe.2019.00099
9. Pranggono, B. and Arabo, A., 2021. COVID-19 pandemic cybersecurity issues. Internet Technology Letters, 4(2), p.e247.
10. U.S. biohackers have "opened" access to insulin. https://openinsulin.org
11.CellPress, 2016. https://www.sciencedaily.com/releases/2016/06/160630135852.htm
12. Mariam Elgabry's written evidence submission to the UK Joint Committee on Biosecurity and National Security. Available at: https://committees.parliament.uk/writtenevidence/6854/pdf/

*"Red-teaming" is an experimental approach of testing the extent of a target system's security and to report any found weakness with the aim to make improvements.

**War crimes were excluded as their prohibition dates back to 1972. They have been regulated by the Biological Weapons Convention (UN 2018a), United Nation Security Council Resolution 1540 (2004), International Health Regulations (IHR) (WHO 2008) & Global Health Security Agenda (2018).

***"Biohackers" have technical experience in innovating, developing or using biotechnologies – they may or may not have a qualification, and practice synthetic biology outside of an institution.

Our research
This work was carried out by the Dawes Centre for Future Crime at UCL. This briefing was produced in partnership with Florence Greatrix at UCL STEaPP's Policy Impact Unit. The research was funded by the Dawes Centre for Future Crime at UCL.

Lead researchers
Mariam Elgabry, PhD, Cyber biosecurity, Lead author and researcher, Dawes Centre for Future Crime
M.Elgabry.17@ucl.ac.uk; www.mariamelgabry.com

Professor Shane Johnson, Principal Investigator, Dawes Centre for Future Crime shane.johnson@ucl.ac.uk

Contact us
https://www.ucl.ac.uk/jill-dando-institute/research/dawes-centre-future-crime
https://www.ucl.ac.uk/steapp/collaborate/policy-impact-unit-1