Gene Synthesis Security

Introduction

The vision behind gene synthesis is to rapidly build any desired genetic sequence, whether it is found in nature or dreamed in our imagination.[1] Each week, researchers from around the world order custom DNA sequences from dozens of international gene synthesis providers. These sequences are used to test ideas for innovation, making gene synthesis critical for growing America's biotechnology industry.[2] This work is increasingly feasible thanks to a competitive marketplace of providers lowering costs, resulting in a widening set of individuals who can turn their genetic blueprints into reality and contribute to groundbreaking advancements.[3]

The responsible advancement of this industry includes understanding when there needs to be more concern over the process of synthesis. Gene synthesis security involves understanding a) whether the combination of sequences or the customer ordering them is concerning, b) whether the sequences printed match what was ordered, and c) who is responsible for acting when concerns arise. Additionally, as artificial intelligence (AI) increases our ability to engineer biology, there are concerns that machine-learning tools could be used to design DNA sequences that are harmful but do not look like any sequence we have ever seen before. While it is unclear if or when this will become feasible, it would outmatch our current ability to identify sequences of concern.

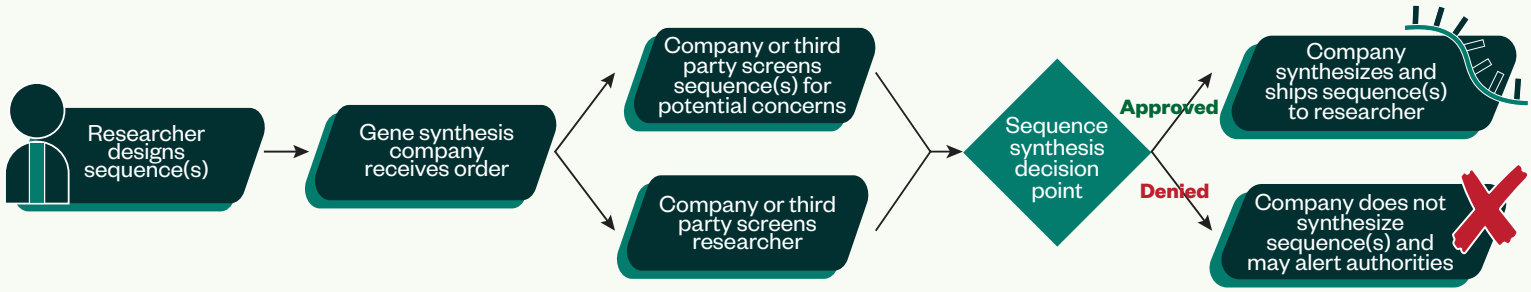
Synthesis screening challenges

The best approaches to gene synthesis security have been debated for nearly two decades.[4] To date, the U.S. Government has remained largely advisory and narrowly focused on sequence and customer screening instead of the larger synthesis security landscape. In current best-case scenarios, a customer orders a sequence that is then screened against an internal database, with customer follow-up conducted on a case-by-case basis (see figure below). However, this process is not required or standardized and there are many cases where screening does not occur.

Currently both the Executive Branch and Congress[5] are working on institutionalizing gene synthesis screening, which could help to address the challenges:

There is no universal consensus on the set of sequences that merit concern, beyond those known to code for certain pathogens: Current screening databases typically include sequences either because they represent partial code of known pathogens and toxins, or because of other security, ethical, or proprietary reasons. Which part of those sequences is concerning, and how to determine the level of concern for novel sequences, is an active area of debate. For example, determining the appropriate level of concern may vary depending on which parts and how much of a virus's genome a customer orders.

Generalized gene synthesis order process



There is no unified screening process: The 2023 screening guidance issued by the U.S. Department of Health and Human Services (HHS)[6] and the 2017 guidance issued by the International Gene Synthesis Consortium (IGSC),[7] are not identical, and both are voluntary.

There is no codified mechanism for alerting officials: The HHS guidance suggests that providers not fill orders that raise concerns from a screening process and report the orders to the FBI. No action is currently required by law if a provider receives a potentially concerning order.

Challenges beyond screening sequences and customers

Several aspects of synthesis security beyond screening sequences and customers also merit closer attention:

Gene synthesis screening will not address sophisticated actors: No screening system is likely to stop a sophisticated state or non-state actor, who could simply synthesize their material outside of commercial providers. Screening will likely be most effective in catching accidental orders of sequences of concern or unsophisticated actors attempting to directly acquire genetic material to cause harm.

Little enforceability and visibility: The Federal Government and synthesis organizations could benefit from a shared understanding of what synthesis organizations are doing in practice to ensure security. This should be done to ensure that all organizations, even those in the IGSC, engage in effective screening practices.[8]

Gene synthesis security does not account for emerging risks created by AI: Advancements in AI capabilities could make it easier to design concerning sequences that bypass existing screening protocols. This is likely beyond the capabilities of the convergence between AI and biology today but could be possible in the future.[9] Addressing this will rest on the ability to collect new biological information that better describes the link between genetic sequences and functions, and a way to rapidly screen new sequences against this expanded dataset. Both processes may themselves benefit from AI advances as well.

Domestic gene synthesis security does not immediately address global implementation: U.S. legislation mandating screening standards would set a valuable precedent. However, in isolation it could simply drive customers and providers towards countries without screening regulations.

Inability to address machine tampering: There are currently no standards for ensuring the physical and operational security of gene synthesis capabilities, including device standards and sequence databases. This leaves individual providers to determine best practices and gives the Federal Government limited insight into how each organization balances economy, security, and other priorities.

Proliferation of benchtop devices presents additional challenges: The growth in the number of smaller benchtop gene synthesis machines could make it easier to bypass existing screening protocols.[10] The length of genetic sequences that can be synthesized with these devices is projected to overlap with the length of the smallest viruses in the next two to five years.[11]

By engaging proactively with stakeholders, including government agencies, gene synthesis providers, and customers, policymakers can consider expanding the United States' capabilities to guard against threats of misuse while promoting economic competitiveness and the open exchange of information.

Sources

1 The National Security Commission on Emerging Biotechnology. "DNA 101: Reading, Writing, and Editing"
2 The Nuclear Threat Initiative. "Preventing the Misuse of DNA Synthesis Technology"
3 Carlson, Rob. "DNA Cost and Productivity Data, aka 'Carlson Curves'"
4 Garfinkel, Michele, et al. "Synthetic Genomics: Options for Governance"
5 The White House. "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence"
6 Administration for Strategic Preparedness and Response. "Screening Framework Guidance for Providers and Users of Synthetic Nucleic Acids"
7 International Gene Synthesis Consortium. "Harmonized Screening Protocol v2.0"
8 Kane, Arianne, et al. "Screening State of Play: The Biosecurity Practices of Synthetic DNA Providers"
9 The National Security Commission on Emerging Biotechnology. "AIxBio White Paper 1: Introduction to AI and Biotechnology"
10 The Nuclear Threat Initiative. "Benchtop DNA Synthesis Devices: Capabilities, Biosecurity Implications, and Governance"
11 Service, Robert. "Benchtop DNA printers are coming soon—and biosecurity experts are worried"

For any questions about this white paper, or related work at the National Security Commission on Emerging Biotechnology, please contact us at ideas@biotech.senate.gov.

Staff at the National Security Commission on Emerging Biotechnology authored this paper with input from the expert Commissioners. The content and recommendations of this white paper do not necessarily represent positions officially adopted by the Commission.