nature communications

Perspective

https://doi.org/10.1038/s41467-024-55436-y

The need for adaptability in detection, characterization, and attribution of biosecurity threats

Received: 15 August 2024

Accepted: 12 December 2024

Published online: 19 December 2024

Check for updates

William Mo[1,2], Christopher A. Vaiana[3] & Chris J. Myers[2]

Modern biotechnology necessitates robust biosecurity protocols to address the risk of engineered biological threats. Current efforts focus on screening DNA and rejecting the synthesis of dangerous elements but face technical and logistical barriers. Screening should integrate into a broader strategy that addresses threats at multiple stages of development and deployment. The success of this approach hinges upon reliable detection, characterization, and attribution of engineered DNA. Recent advances notably aid the potential to both develop threats and analyze them. However, further work is needed to translate developments into biosecurity applications. This work reviews cutting-edge methods for DNA analysis and recommends avenues to improve biosecurity in an adaptable manner.

Recent advances in biotechnology significantly elevate the risk of malicious applications. The 21st century to date has already featured multiple examples of problematic biological threats. Most infamously, the COVID-19 pandemic's impact was severe and universal, causing economic issues and flaring political tensions in many countries[1]. Additionally, the 2001 anthrax attacks in the United States illustrate the potential threat of bioterrorism[2]. Anthrax is, among toxic substances, relatively easy to grow and store, and it was very difficult to locate and detain the perpetrator. Furthermore, the investigation was not fully conclusive and is mired in significant controversy[2]. As biotechnology becomes increasingly more powerful and accessible, the prospect of a threat that possesses both the devastating potential of a pathogen and the elusiveness of a manufactured toxin is in turn increasingly more viable[3,4]. *Biosecurity* is a set of preventative measures that aim to recognize and control potential manmade biological threats, in order to minimize the damage inflicted upon human life and society. The potential risks of such threats have greatly increased in recent years as dedicated synthetic biology research yields better methodologies which reduce costs and increase reproducibility. The financial and educational entry barriers to both gene editing and gene synthesis have substantially lowered, enabling great benefits for healthcare, ecology, agriculture, and more[5–7]. However, malicious applications of the same methods could also inflict havoc in these areas and extensively debilitate infrastructure[8]. Biosecurity struggles to keep up-to-date with ever-improving methods[9], and, fortunately, there has not yet been a major incident involving engineered DNA that can be used as a case study. Without the benefit of hindsight, biosecurity must match the newfound breadth of potential engineered biological threats with an equally broad set of countermeasures. A 2018 report from the National Academies noted that the most immediate threats involve leveraging existing understood pathogen genomes and metabolic pathways with small-scale alterations to either increase pathogenicity or toxicity, or to enable more efficient production of dangerous substances[10]. In the years since, the threat landscape has most notably evolved with the advent of *artificial intelligence* (AI) models, particularly tools for generative protein design like RFDiffusion from the lab of 2024 Nobel Prize winner David Baker[11–13]. The recent Executive Order 14110 identifies biosecurity as a major risk factor amongst others in AI, prompts a currently in-progress National Academies biosecurity study on AI to complement the 2018 one, and directs action towards better regulation of AI use in biodesign, but it is unknown what degree of enforcement will manifest, what existing or new government agency would be responsible, and if the order will remain in effect in future administrations[14]. In addition to apt consideration of present risks, biosecurity frameworks must be forward-facing in their adaptability in order to match the potential

[1]Draper Scholar, The Charles Stark Draper Laboratory, Inc., 555 Technology Square, Cambridge, MA, USA. [2]Department of Electrical, Computer, and Energy Engineering, University of Colorado Boulder, 1111 Engineering Dr, Boulder, CO, USA. [3]The Charles Stark Draper Laboratory, Inc., 555 Technology Square, Cambridge, MA, USA. e-mail: chris.myers@colorado.edu

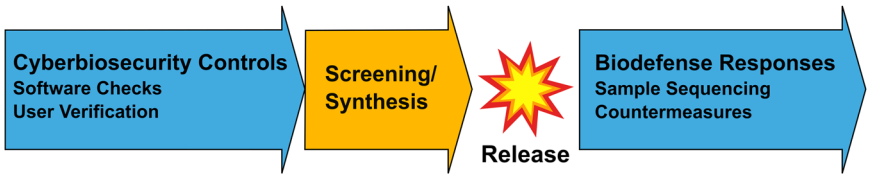

Fig. 1 | Chronology of a biosecurity threat and appropriate responses. Defining the "boom" or event that compromises safety as the release of a dangerous biological agent, there are "left of boom" and "right of boom" security measures. Highlighted in orange, screening of engineered sequences is a developed and focused area in biosecurity. In blue, more proactive measures to limit actors in the design phase, as well as more efficient ways to respond to an already-released agent are areas that should be further developed.

threat space that will grow to contain more diverse yet specialized forms of attack as bioengineering capabilities improve.

Currently, a major focus in biosecurity is on screening sequences sent to companies that synthesize DNA to order[15]. This is a very efficient point of containment, since accurate sequence information is available for analysis at this stage. However, DNA screening has significant limitations. In the present day market of DNA synthesis, different companies employ different protocols for screening, with the details of each not being public and a lack of rigid standards[16]. Recommendations issued by the US Department of Health and Human Services (HHS) were recently updated to address shortcomings raised in several essays and studies[15–17], but still do not comprehensively detail or enforce many specific restrictions[18]. The *International Gene Synthesis Consortium* (IGSC)'s Harmonized Screening Protocol attempts to be more comprehensive, but its only real update since 2009 mostly clarified merely that smallpox should not be synthesized[16]. No protocols are universally accepted or enforced, resulting in potential weak links for malicious actors to exploit[16]. Meanwhile, AI accelerates both the dispersion of potentially misusable knowledge related to biology and biosecurity[19] and the capabilities of de novo threat design[11,20]. While creating entirely original threats is presently difficult, it is already plausible to use current AI methods to engineer small changes to existing templates with potentially devastating results. One example would be the use of a prediction model like EVEscape[21] to deliberately engineer a pathogen mutation for immune escape. The state of DNA screening at present is ill-equipped to handle malicious actors who can easily discover from *large language models* (LLMs) how to circumvent screening by ordering from non-IGSC providers[19] and attempt to synthesize sequences that encode novel dangerous proteins. Furthermore, next-generation benchtop DNA synthesis devices[22] are not being designed with built-in screening protocols, and may be vulnerable to firmware attacks that disable such precautions anyway[23]. While air gapping DNA synthesis devices may seem like an obvious solution, the need to constantly update screening databases and methods to detect the latest novel threats makes this a challenge. With such limitations in mind, it is clear that even in a future with effective and widespread screening standards, potential workarounds will still exist.

To help ensure robustness in biosecurity practice, effective and alternative checkpoints are necessary. For example, software design tools could add automated checks that catch, warn the user of, and catalog for future reference harmful DNA sequences during their development. In addition, design tools and synthesis companies alike could enforce stricter user verification methods. Existing types of security would describe these measures as "left of boom", or deterrents that occur before engineered DNA is used maliciously (see Fig. 1)[24]. As these methods involve computer analysis and surveillance, such work overlaps with cryptography and cybersecurity, and can be more clearly defined as "cyberbiosecurity"[25,26]. Following deployment, being able to sample and identify engineered DNA sequences from the environment they are present in and accurately evaluate their purpose and origin is also important in order to determine the best response. Such measures that happen "right of boom" can be considered "biodefense"[10]. Developing better tools both left and right of boom alongside the improvement of current screening methods is important to help ensure a more airtight set of protocols. By covering such a broad set of bases, a comprehensive biosecurity suite can also serve as a more effective deterrent against malicious actors. In order to manifest such a comprehensive biosecurity portfolio, better solutions to current problems in the analysis of engineered DNA are necessary. These methods do not have to be developed from scratch, however, as the same biotechnology advances that promote greater biosecurity risks also necessarily enable the development of superior biosecurity tools.

Review of analysis methods

As depicted in Fig. 2, this paper focuses on three key biosecurity problem statements involving engineered DNA: (1) detecting the presence of unknown engineering in sampled DNA, (2) characterizing the function and purpose of engineered DNA, and (3) attributing engineered DNA to its origin. Analysis methods that solve these problems will be essential to formulating effective countermeasures to maliciously bioengineered agents, as unique customization within the vast potential threat landscape necessitate any response to be equally tailor-made. Within the review of relevant previous work, the most critical observation is that adaptability is necessary for biosecurity to keep pace with new scientific developments and fit real-world needs.

Detection

In right-of-boom scenarios, being able to identify that engineered organisms or viruses exist in key clinical or ecological environments is an essential first line of defense[27]. This need arises in both reactive and proactive cases where sequencing can already be employed to characterize natural DNA. Reactive cases involve DNA sequencing in response to an observable change, such as in diagnosing visibly sick patients[28] or troubleshooting low crop yields. Proactive cases, on the other hand, rely on routine screening events such as water or food supply inspection[29]. Proactive scenarios pose a somewhat more difficult detection problem, since signs of DNA engineering cannot be tied to any yet noticeable problems. Still, any situation where the presence of unknown engineering is detected raises immediate red flags and both prompts and enables further analysis. The detection problem statement in a more general form predates the modern synthetic biology landscape, as concerns can be found in the literature dating back to the 1980s about engineered bacteria[30], with similar questions being asked in intervening decades[31]. It has also been tackled by researchers interested in detecting *genetically modified organisms* (GMOs) in agricultural yields for the benefit of those fearful of consuming such products[32–34]. This problem is nevertheless very much unsolved due to a variety of challenges faced at several stages. First accurate sequencing reads must be captured from noisy environments, then abnormal reads associated with engineerable genomes must be filtered out from the larger dataset, and finally the abnormal reads must be analyzed to identify them as containing engineered sequences. Moreover, the vast variety of potential environments to survey include several types of human tissues, wastewater, soil, food supplies, and more[35]. Each unique environment features different

https://doi.org/10.1038/s41467-024-55436-y

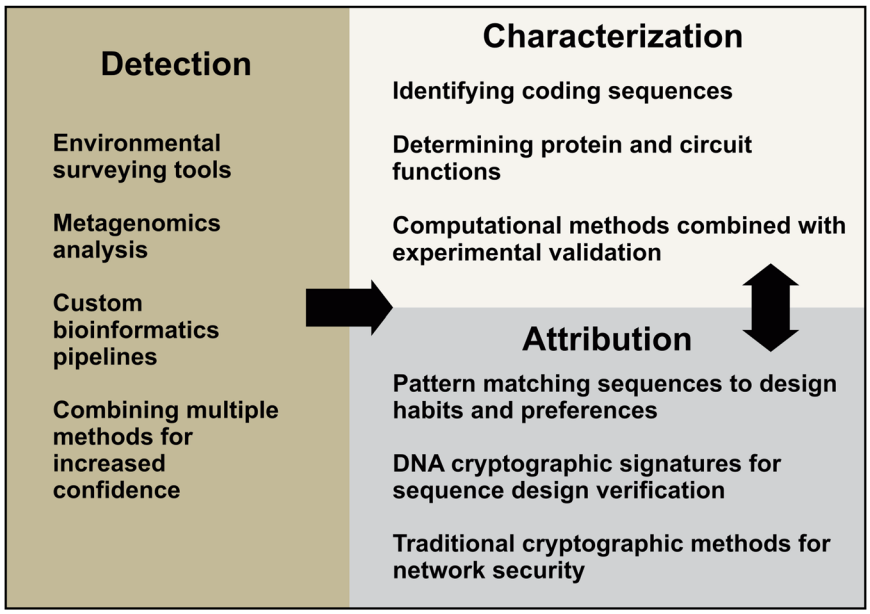

Fig. 2 | Workflow of biosecurity agents in response to potential engineered threats. When faced with real-world situations with many unknown variables, detection methods establish if there is an engineered element that needs further investigation. Following this, characterization methods help determine the properties and purpose of the agent, while attribution methods help establish its origin. Characterization and attribution work can happen in parallel and their outcomes can aid the other.

physical challenges and organisms, further complicating the problem and hindering a universal solution.

A recent *Intelligence Advanced Research Projects Activity* (IARPA) program named *Finding Engineering-Linked Indicators* (FELIX) focused heavily on the detection problem, with the methods used varying between different groups[36]. Some work funded by FELIX aimed to improve the first step by prototyping an advanced portable sequencing kit that can amplify markers of genetic engineering[37]. However, this work is currently unpublished and this step of the problem is overall in need of much more focus. The second step, identifying rare abnormal reads from an enormous dataset, is tied to metagenomics, an adjacent but highly relevant field of research. Metagenomics focuses on accurately distinguishing between the sources of different DNA reads and sequences when taking a sample from a broad environment rather than a controlled subject[38], forming a critical first step in identifying potential engineered DNA. Most metagenomic studies focus on ecological diversity and microbiome composition, but a significant amount is nevertheless closely linked and could be adapted to biosecurity purposes[39,40]. For example, several instances of clinically-inspired metagenomics work involve detecting pathogens from patient tissue samples using *next-generation sequencing* (NGS) data, in place of more traditional biopsies or chemical tests used to diagnose certain pathogen-caused illnesses[28,41–43]. Metagenomics is thus capable of identifying unusual DNA sequences with high sensitivity and specificity within clinically-relevant samples[43]. In a future where such a flagged sequence may signify an engineered agent of biological attack, this is extremely valuable to biosecurity. However, more investment is needed to be able to enable accurate metagenomic analyses in as many unique sampling environments as possible where threats could be found[35]. Fine-tuning of the thresholds to flag suspicious reads is also necessary to avoid either too many false positives to review or too many false negatives ignored in the context of what will always be an extremely noisy sample[44]. When fully developed to be adaptable to numerous contexts, metagenomic methods can serve as a key initializing step in a flagging protocol that provokes more detailed examination and whole-genome sequencing and analysis of suspicious samples[45]. This produces an ideal starting dataset of suspicious reads with maximum context and minimum contamination for downstream computational approaches[46,47].

Other FELIX work focused on these downstream computational approaches in a variety of contexts and organisms. One group demonstrated the use of simulation-trained neural networks to detect genetic engineering in the relatively malleable genomes of model prokaryotes[48]. This approach targets prokaryotes because they have less complex epigenetic and regulatory interactions than multicellular eukaryotes, such as humans, resulting in a high quantity of possible edits. The authors chose to use a neural network trained to scan for numerous unique genetic patterns at once and confidently identify the presence of specific types of edits. These edits are representative of what various labs might do, such as genetic region inversion, gene deletions both full and partial, and insertion of fluorescent proteins[48]. Other work focused specifically on yeasts, important model organisms in genomic work and biomanufacturing applications[49]. One research group built a bioinformatics pipeline known as Prymetime that could assemble yeast genomes from *whole-genome sequencing* (WGS) reads and simultaneously detect and annotate signs of genetic engineering. This pipeline allows a user to evaluate if a given sample may have been engineered by an unknown party to either test some form of eukaryotic genetic design or produce a desired substance[49]. While the recent work in detection of engineered DNA is very promising, there exist some shared limitations that highlight the most pressing needs in this space. These limitations broadly manifest in the form of over-specificity; rigid methods typically work only for specific organisms, require specific assumptions about the sample to return accurate results, and perhaps most importantly, can only detect specific kinds of edits with known key features. The next big advances in this challenge should manifest in the form of more flexible computational tools that can be continuously updated and expanded. An example of such an approach is the tool GUARDIAN, created by several of the same researchers behind Prymetime[50]. GUARDIAN incorporates a collection of detection methods and combines their results together to get a more reliable consensus on if a sample is engineered[50]. Although this approach still has some limitations, such as only being able to reliably detect genetic inserts, modularization of the individual components in GUARDIAN

and standardization of how their results are communicated enables more extensions, modifications, and incorporations of other methods going forward[50]. This is an example of the kind of adaptable approach that is necessary to match the rapid progress made in biotechnology and biosecurity policy developments going forward.

Characterization

Determining the purpose or function of engineered DNA detected in the environment, or any DNA being ordered for synthesis, is needed in order to perform an accurate threat assessment. Current DNA screening methods focus on identifying hazardous or pathogenic sequences, the most immediate and dangerous threats. However, some engineered DNA may not immediately appear to encode any destructive or adversarial function. Characterization also includes more advanced understanding of the genetic context that the DNA operates in. These subtler aspects of characterization are important when considering that some biological threats, such as a pathogen with an asymptomatic phase, could propagate without causing significant immediate impact. The simplest way to understand any whole is to understand each of its parts; this logic can be applied to engineered biology, and thus identifying specific genetic parts in an engineered sequence is an essential starting point. This facet of the characterization problem is manifest in DNA screening; sequences submitted for synthesis must be rigorously examined to determine if they encode anything particularly dangerous. Detecting the parts used in the construction of engineered DNA can critically highlight dangerous functions. This can be accomplished in several ways, the most basic being to simply run a full-scale best match search using algorithms such as BLAST against a list of pathogen genomes[18]. However, it is important to have more precise and extendable methods, which can identify specific genetic parts associated with virulence or pathogenicity while filtering out large, mostly harmless sequences, and then utilize these annotated parts in downstream analysis. The foundations for such methods are likely to come from the synthetic biology community itself, because there is already a vested interest for designers to have convenient tools for identification and annotation of specific genetic parts[51]. One notable example of such a tool that is open-source is PlasMapper[52]. Originally published in 2004, it has undergone significant revisions with the most recent updated version, 3.0, being released and published in 2023. Focused on plasmid design, its goals are oriented around clear web-based annotation and visualization of plasmid sequences to help users understand and identify key elements in their cloning vectors[52]. Other tools built around slightly different goals can produce annotated files in the GenBank or *Synthetic Biology Open Language* (SBOL) formats, which are more robust at capturing key sequence information[51,53]. These tools can be adapted to focus specifically on identifying potentially dangerous genetic parts and form a framework for detailed computational analysis of the offending sequence.

As the primary focus of current screening approaches, the characterization problem also needs the most amount of work dedicated to preventing deliberate subversion, such as by using de novo proteins or the masking of malicious coding sequences. One example of a novel and efficient DNA screening method that is specifically open-source, and explicitly tackles the risk of malicious actors deliberately obfuscating the dangerous elements of their sequences, is that of *random adversarial threshold* (RAT) screening[54]. RAT screening demonstrated effectiveness at stopping theoretical malicious synthetic biologists from sneaking past screening in a "red team" simulation. Notably, this method specifically relies on pregenerated predictions of potential variants and subsets of dangerous coding sequences. A key limitation is that if the capability of the "red team" to predict how to accurately modify sequences without losing functionality significantly exceeds the capability of the biosecurity protocol they are trying to breach, then their chances of success improve significantly[54]. This observation further underscores the importance that biosecurity methods need to be built on a foundation that is continuously adaptable to the latest discoveries and approaches, but also reinforces the positive point that knowledge is power, and advances in biodesign naturally lead to potential advances in biosecurity.

In the particular case of a dangerous de novo protein design, characterization analysis bears the burden of not only identifying the coding sequence within the DNA but also attempting the extraordinarily difficult task of figuring out what the protein actually does. Sequence-to-function prediction faces many challenges even when only looking at natural proteins, as the most straightforward approach of homology-based methods encounters numerous difficulties due to small sequence or structure differences yielding tremendously different functions[55]. Characterizing de novo designed proteins adds yet another layer of complexity, especially as they can now be generated from AI approaches[11,20]. One proposed way to logistically simplify this problem enormously is to ensure that all de novo protein design generation is monitored and cataloged, and continuously update screening databases accordingly[56]. However, as with screening itself, achieving this level of consensus regulation could end up being highly challenging. When directly faced with the problem itself, some neural network approaches, particularly *convolutional neural networks* (CNNs), have shown promise to predict de novo structure and function with reasonable accuracy[57]. One such tool is DeepGOPlus, which notably can be tweaked to search only based on motifs, enhancing its potential for analyzing relatively unknown or novel sequences[58]. However, it also does not account for protein interaction networks, which could limit its ability to identify a protein engineered to target a specific pathway or binding site[58]. Once again, as AI methods evolve in general to enable superior threat design by way of generating sequence from function, they should also enable superior threat analysis by way of generating function from sequence. However, this field of work still has a long way to go, as existing methods currently have limitations and are not optimized for the specific task of detecting potential engineered threats. Sometimes direct characterization of the resulting protein outcomes, such as by examination of a patient infected by a biological threat, will be necessary.

Beyond recognizing coding sequences of concern, another helpful part of characterizing suspicious engineered DNA is to understand functionality details. A useful analogy to draw here is to that of *improvised explosive devices* (IEDs), contemporary security threats highly relevant today due to the abundance of chemistry and instrumentation knowledge and materials. IEDs can be built using electrical circuits to trigger under certain criteria. In the future, a biological threat can similarly be configured using increasingly advanced synthetic biology methods, but simply identifying the circuit in question is significantly more difficult than the IED equivalent of physical examination. Computational methods exist to predict genetic circuit structure from a sequence[51], and can be further sharpened with a focus on dangerous sequences. However, in the absence of rigid test parameters representing fully characterized phenomena that anchor simulations in other disciplines, simulation of the phenotype associated with unknown genetic engineering can be unreliable in even the highest quality in silico methods. As with the analysis of protein outputs, experimentally evaluating the properties of unknown DNA can elucidate genetic circuit mechanisms. The ideal approach here is akin to testing an electrical circuit with specific inputs and outputs in order to collect more practical data on function[59]. However, it is very difficult to design a workflow or platform to do this that is applicable in multiple contexts, especially unknown contexts, because divergent evolution has led to an enormous number of incompatibilities in interactions between different biomolecules. Furthermore, it is difficult simply to control the exact inputs of such an experiment precisely while minimizing confounding variables[60]. One notable example of careful control of inputs and measuring outputs in a genetic circuit

involved adding promoters controlled by light to a genetic circuit and characterizing the resulting optogenetic circuit behavior based on analog light input signal strength[59]. In an analogy to electrical circuits, light-controlled oscillation generated waveform outputs, mirroring the use of a function generator and oscilloscope[59]. Other work implemented a cell-free system to induce circuit behavior independent of confounding factors from a live cell[60]. This significantly reduces the complexity of the experimental model for the circuit, while still preserving the ability to test how varying certain key parameters could influence gene expression output. The cell-free platform was emphasized as being a biological equivalent to a breadboard, as opposed to a function generator and oscilloscope, when those elements are often used in tandem to test electrical circuit designs[60]. Each of these two platforms is focused on facilitating design, but the concepts used also have the potential to be used for reverse engineering such designs. Both papers were also published in 2014, before numerous recent advances in synthetic biology and design. Although both have been highly cited in optogenetic and cell-free research, respectively, there is a gap in discovering the feasibility of applying these concepts to characterize an initially unknown genetic circuit, rather than testing and iterating on a purpose-built circuit.

Finally, a greater understanding of the context surrounding suspicious DNA sequences could plausibly be elucidated by identifying the methods by which it was designed and assembled. This is, however, an extremely difficult task as increasingly popular and accessible methods like Gibson assembly tend to not leave noticeable scars[61], and the best that can be done is to try and identify certain areas that are associated with enabling certain kinds of edits; for example, the PAM sites specific to various Cas9-based platforms[62]. Furthermore, there is a lack of existing work that has focused on reliably demonstrating the ability to identify methods of assembly. This is a risky avenue of work as advances made in it are more likely to be overly specific and swiftly obsoleted by newer methods. Biosecurity approaches deriving from synthetic biology design as discussed above are more promising, as they can be more easily extended alongside developments in the original tools.

Attribution

Determining individual and sometimes vague characterizations of engineered DNA does not necessarily inform biosecurity experts on how to counteract a possible threat. Instead, detective work can potentially yield more conclusive results by discovering the origin of a suspicious sequence. By scanning for specific details that include not only certain overall build approaches as well as smaller details like promoter choice that are often innocuous independently, these small associations and clues can collectively form a best guess picture of who engineered the sequence in question[63]. This again can be compared to the case of IED threats, where certain patterns in the construction of devices could be considered hallmarks of a particular individual or organization. This problem is not necessarily a follow-up to the characterization problem, but rather one that can be tackled in tandem. Improvements in and insights gained from characterization can narrow down some of the detective work involved in attribution. At the same time, attribution can indirectly lead to better characterization. Correct identification of a creator can lead to an immediately greater understanding of the nature of engineered DNA when considering the history of the creator's work. However, attribution comes with extreme sensitivity risks, as false accusation can lead to inflamed tensions and increase mistrust. Specific controls in DNA sequences explicitly designed to validate the identity of the creator can be extremely useful for avoiding these situations.

Recent work has demonstrated an important foundational step in detecting the lab-of-origin of an unknown sample[63]. This approach involves the use of training a deep neural network to categorize engineered sequences. The training and validation datasets were taken from Addgene sequence databases, beginning by selecting labs with a significant number of publicly available sequences and from there randomly selecting some sequences from each lab for either training or validation. The authors were able to demonstrate that their trained neural network could include the true lab-of-origin in its top 10 predictions more than half of the time, marking a decent accuracy standard that with improvement could be of great help in biosecurity[63]. Other work has sought to make more advances in neural network approaches by incorporating additional features of sequences to categorize, like phenotypic metadata[64,65]. These methods are effective and possibly highly future-proof as machine learning in general develops, but could run into application issues because of how it may be difficult to determine exactly why a given lab-of-origin is highly predicted. An alternative approach proposed an algorithmic solution to the lab-of-origin problem in place of neural networks[66]. Their tool, dubbed PlasmidHawk, also utilized the portfolios of labs with a high number of publicly available Addgene sequences. However, PlasmidHawk focuses on aligning a test sequence to a highly expansive pan-genome assembled from all synthetic sequences in the training dataset, and then identifying the most likely lab-of-origin based on the greatest number of successful alignments of significant sub-sequences of the test sequence. They reported overall greater accuracy of prediction over neural network approaches and were able to expand upon their analysis of prediction instead of having to deal with an intrinsic black box[66]. However, their work may also be more susceptible to becoming outdated as engineering methods evolve and neural network approaches are able to more effectively compensate by utilizing additional parameters[64].

As multiple approaches to the lab-of-origin problem with different strengths and weaknesses continue to be developed, it is highly plausible that, as with traditional forensic work, the results of multiple analysis tools and tests can be utilized together to determine a most likely culprit. This is much like how the detection problem can be tackled using a concatenation of tools. However, fundamental limitations to all of these methods can still impede an investigation. For example, simply relying on sources like Addgene for designer patterns is a flawed assumption in the real world as one could reasonably assume that malicious actors will not publish their work in such public resources. Rather, it is possible to easily mask the true creator of a sequence by methods such as swapping a less important genetic part for a largely equivalent part primarily used by and thus strongly associated with another lab[63]. This would be an easy way to create a false red flag and frame others. It is precisely for this reason that the attribution problem includes not only the tracking of malicious actors, but also the verification of proper ones[67]. There are existing standards and methods for ensuring that labs working with particularly hazardous biological materials are trustworthy[68], and these could be extended to aid the logistic side of biosecurity attribution.

User verification methods analogous to other security fields are enabled by the ability to leverage cryptography and its methods upon DNA data[69]. In particular, digital signatures can be implemented into non-coding DNA for the purposes of proper attribution; a specific section of sequence can be used to validate authorship by a particular person or organization[70]. This can lead to two distinct advantageous flagging scenarios in biosecurity. First, if a DNA signature appears in a sequence not claimed by the author of the signature, then the sequence may have been stolen or otherwise misused. Second, if a trusted author submits a sequence that does not contain their signature or contains a corrupted signature, this indicates that their computer system may have been compromised by an outside cybercriminal using their credentials to synthesize a threat, a notable novel angle of biosecurity attack[26]. This can help resolve and expedite security concerns associated with researchers conducting properly supervised and safe research on dangerous biomaterials. It also simultaneously provides a quick way to identify engineered sequences

of very serious concern, as the stealing or spoofing of a sequence is a behavior likely to be associated with that of a malicious actor. There exist, however, some technical barriers with the technology, such as potential loss of function associated with inserting necessarily hundreds of base-pair length signatures into DNA, and the risk of mutations compromising the integrity of the signature. Additional work has sought to create DNA signature methodology that reduces these limitations, but still experiences some signature validation failures in their experimental results due to factors such as low sequencing quality leading to failed assembly[70]. As there can be serious consequences to get even a single detail wrong in cryptography, more work to expand upon and ensure near 100 percent reliability could increase the vaiability of this approach. However, there are also fundamental external barriers against cryptographic signature verification to consider, such as arguments over copyright and IP protection of genetic parts versus open source and the reproducibility of work that could benefit science as a whole[71].

The issue of author verification can also be tackled from a more traditional cybersecurity standpoint. RAT screening is part of the initiative behind, and has been incorporated into, SecureDNA, a platform designed to facilitate universal, efficient, and effective biosecurity screening[72]. SecureDNA includes significant consideration for the privacy of users, employing cryptographic techniques to minimize the risk of potential trade secrets being leaked while still ensuring that thorough hazard screening is conducted. It also critically contains provisions for users with verified credentials and authorization to work with hazardous biomaterials to efficiently bypass the flags that their sequences will raise when screened[72]. This is an example of a useful early step in securing the biodesign process from a baseline computational level, but there is still a serious lack of widespread adoption of such methods.

A final concern about the creator of a sequence involves the use of AI by a designer without significant biological expertise. Currently, AI use in biodesign is primarily used by experts in areas like de novo protein design[11,20] and metabolic engineering[73–76]. However, it is possible that AI use in the future could reach a point where an individual could gain significant knowledge about biosecurity weaknesses from LLMs[19] and generate complete genetic designs according to vague initial specifications[77,78]. This particularly lowers the barrier of entry involved and raises the risks of an uninformed individual creating and ordering something that is dangerous, perhaps without even them realizing it. If AI is relied upon to generate entire circuits, it also may plausibly do so by referencing machine-accessible data from literature and public databases, thus producing attribution patterns that will resemble existing, legitimate researchers. By building tools specifically oriented towards detecting that AI was involved in the design of a DNA sequence, more specific questions could be leveraged to inform regulators about the risks of AI use in biodesign as well as determine the capabilities and motivations of the human behind the design. In other fields where the use of AI has led to controversy, including education and the arts, it has been found that separate neural networks trained to detect work produced by AI can be fairly accurate at doing so, though this could easily change[79]. Should AI tools evolve into a viable state such that even an uninformed individual could use them to engineer dangerous DNA sequences, biosecurity researchers should probe whether such classification outcomes are also true when said work manifests as DNA sequences, and do so continuously to be thoroughly aware of current capabilities.

Discussion and recommendations

The production of engineered DNA and resultant products is becoming increasingly accessible as synthetic biology methods improve. While this presents an optimistic outlook on how humanity could benefit from such work, biosecurity is in danger of seriously falling behind the curve in the creation of tools that can accurately counteract more malicious applications. A significant amount of present biosecurity research is leveraged specifically at the screening process prior to a company's synthesis of ordered DNA. While screening is an important and effective funnel point for biosecurity focus, it is not infallible, and research should be targeted at improving methods and protocols applicable not only in screening, but before and after to build a modern, robust biosecurity portfolio. The primary recommendation of this work is that modern biosecurity methods need to be highly adaptable, both to fit within a security framework with multiple checkpoints and to keep pace with the rapid evolution of biotechnology and real-world concerns.

Building such a broad and flexible shield is not an endeavor that needs to be started from scratch. This work has shown that relevant expertise and knowledge can and should be derived and translated from work in related subjects. The pieces for biosecurity to keep pace with biotechnology are available, and necessarily will be in the future, but work needs to be put in to assembling these pieces into a functioning whole biosecurity strategy that builds upon the foundation of current screening methods. In the detection problem, combining dedicated sampling hardware, metagenomic analysis, and effective classification software into a cohesive, modular workflow is a key goal. In the characterization problem, the same synthetic biology methods that make genetic engineering more accessible to malicious actors are also sturdy skeletons that should be fleshed out into reverse-engineering tools for threat assessment. In the attribution problem, concatenating different software approaches to identifying sequence lab-of-origin could sharpen the ability to attribute sequences, while cybersecurity can be developed to aid user verification via both DNA-based cryptography applications and traditional computer security.

Three major real-world challenges loom in the future of biosecurity that demand protocols be adaptable enough to avert disaster. First, biosecurity awareness has raised given recent events[80], but this also biases risk assessment towards human pathogens. While an engineered pandemic is the biggest immediate threat given current bioengineering capabilities, dangerous applications of genetic engineering in the future might include other forms of attack, such as an invasive and pesticide-resistant weed that aggressively populates and drains nutrients from agricultural fields. Therefore, methods ideally should be quickly translatable across different species and types of organisms. Second, malicious actors can aim to specifically break biosecurity measures. The characterization problem already faces the risk of actors sneaking dangerous sequences past the current primary focus of screening, leading to developments like RAT screening[54]. Anticipating biosecurity-conscious attacks and devising appropriate backup solutions to them is critical to staying ahead of the potential threat curve, and further demands that biosecurity methods be continuously extendable. Finally, the standardization of tougher biosecurity mechanisms may hassle customers and drive them towards less restrictive competitors, including foreign exporters in the absence of international convention, as seen in previous regulatory efforts such as environmental regulations[81]. In order to reach the compromises that satisfy the economic and political spheres, biosecurity methods again must be appropriately adaptable. Fortunately, proper implementation of any degree of consensus enforcement can serve as a strong deterrent. It is possible to create biosecurity protocols that meet these demands and can naturally evolve in capability alongside biotechnology itself. However, doing so will require an expansion of current biosecurity focus to enlist the expertise of relevant adjacent fields and develop more varied tools with a foundational emphasis on adaptability. In so doing, the safety of humanity can be secured while it reaps the benefits of the great advances made in biotechnology.

References

1. Global economic effects of COVID-19. https://apps.dtic.mil/sti/citations/AD1152929 (2021).

2. Inglesby, T. V. et al. Anthrax as a biological weapon, 2002: Updated recommendations for management. *JAMA* **287**, 2236 (2002).
3. Ahteensuu, M. Synthetic biology, genome editing, and the risk of bioterrorism. *Sci. Eng. Ethics* **23**, 1541–1561 (2017).
4. Melin, A. Overstatements and understatements in the debate on synthetic biology, bioterrorism and ethics. *Front. Bioeng. Biotechnol.* **9**, 703735 (2021).
5. Brophy, J. A. N. & Voigt, C. A. Principles of genetic circuit design. *Nat. Methods* **11**, 508–520 (2014).
6. Jones, T. S., Oliveira, S. M. D., Myers, C. J., Voigt, C. A. & Densmore, D. Genetic circuit design automation with cello 2.0. *Nat. Protoc.* **17**, 1097–1113 (2022).
7. Nielsen, A. A. K. et al. Genetic circuit design automation. *Science* **352**, aac7341 (2016).
8. Wang, F. & Zhang, W. Synthetic biology: Recent progress, biosafety and biosecurity concerns, and possible solutions. *J. Biosaf. Biosecurity* **1**, 22–30 (2019).
9. Millett, P., Isaac, C. R., Rais, I. & Rutten, P. The synthetic-biology challenges for biosecurity: examples from iGEM. *Nonproliferation Rev.* **27**, 443–458 (2020).
10. National Academies of Sciences, Engineering, and Medicine, Division on Earth and Life Studies, Board on Life Sciences, Board on Chemical Sciences and Technology & Committee on Strategies for Identifying and Addressing Potential Biodefense Vulnerabilities Posed by Synthetic Biology. *Biodefense in the Age of Synthetic Biology* (National Academies Press (US), 2018). http://www.ncbi.nlm.nih.gov/books/NBK535877/. **This report lays out a national security perspective on the biological threat landscape as it existed in 2018 and is highly valuable as a reference in consideration of synthetic biology advances, just prior to the biggest surge of AI-based approaches throughout science**.
11. Watson, J. L. et al. De novo design of protein structure and function with rfdiffusion. *Nature* **620**, 1089–1100 (2023). This paper details RFDiffusion, a key example of an AI-assisted tool for de novo protein design which could feasibly be abused by malicious actors.
12. The Royal Swedish Academy of Sciences. The nobel prize in chemistry 2024. https://www.nobelprize.org/prizes/chemistry/2024/press-release/ (2024).
13. Carter, S. R., Wheeler, N. E., Chwalek, S., Isaac, C. R. & Yassif, J. The convergence of artificial intelligence and the life sciences: Safeguarding technology, rethinking governance, and preventing catastrophe. https://www.nti.org/wp-content/uploads/2023/10/NTIBIO_AI_FINAL.pdf (2023).
14. Executive order on safe, secure, and trustworthy development and use of artificial intelligence. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (2023).
15. DiEuliis, D., Carter, S. R. & Gronvall, G. K. Options for synthetic DNA order screening, revisited. *mSphere* **2**, e00319–17 (2017).
16. Diggans, J. & Leproust, E. Next steps for access to safe, secure DNA synthesis. *Front. Bioeng. Biotechnol.* **7**, 86 (2019).
17. Elworth, R. A. L. et al. Synthetic DNA and biosecurity: Nuances of predicting pathogenicity and the impetus for novel computational approaches for screening oligonucleotides. *PLOS Pathog.* **16**, e1008649 (2020).
18. Health {and} Human Services, U. D. Screening framework guidance for providers of synthetic double-stranded DNA. https://www.phe.gov/preparedness/legal/guidance/syndna/documents/syndna-guidance.pdf.
19. Li, N. et al. The wmdp benchmark: Measuring and reducing malicious use with unlearning. https://doi.org/10.48550/ARXIV.2403.03218, https://arxiv.org/abs/2403.03218 (2024). **This paper, a preprint at time of writing and citation, contains a framework that could help researchers address the problem of LLM models empowering malicious actors with knowledge**.
20. Ingraham, J. B. et al. Illuminating protein space with a programmable generative model. *Nature* **623**, 1070–1078 (2023).
21. Thadani, N. N. et al. Learning from prepandemic data to forecast viral escape. *Nature* **622**, 818–825 (2023).
22. Hoose, A., Vellacott, R., Storch, M., Freemont, P. S. & Ryadnov, M. G. DNA synthesis technologies to close the gene writing gap. *Nat. Rev. Chem.* **7**, 144–161 (2023).
23. Carter, S. R., Yassif, J. & Isaac, C. R. Benchtop dna synthesis devices: Capabilities, biosecurity implications, and governance. https://www.nti.org/wp-content/uploads/2023/05/NTIBIO_Benchtop-DNA-Report_FINAL.pdf (2023).
24. Schrier, R. A case for action: Changing the focus of national cyber defense. *Cyber Def. Rev.* **4**, 23–28 (2019).
25. Richardson, L. C., Connell, N. D., Lewis, S. M., Pauwels, E. & Murch, R. S. Cyberbiosecurity: A call for cooperation in a new threat landscape. *Front. Bioeng. Biotechnol.* **7**, 99 (2019).
26. Puzis, R., Farbiash, D., Brodt, O., Elovici, Y. & Greenbaum, D. Increased cyber-biosecurity for DNA synthesis. *Nat. Biotechnol.* **38**, 1379–1381 (2020). This paper excellently illustrates the risks associated with present screening methods and how relatively easy it is to potentially bypass them.
27. Crook, O. M. et al. Analysis of the first genetic engineering attribution challenge. *Nat. Commun.* **13**, 7374 (2022).
28. Bibby, K. Metagenomic identification of viral pathogens. *Trends Biotechnol.* **31**, 275–279 (2013).
29. Acharya, K. et al. Metagenomic water quality monitoring with a portable laboratory. *Water Res.* **184**, 116112 (2020).
30. Ford, S. & Olson, B. H. Methods for detecting genetically engineered microorganisms in the environment. In Marshall, K. C. (ed.) *Advances in Microbial Ecology*, Advances in Microbial Ecology, pp.45–79 (Springer US, 1988). https://doi.org/10.1007/978-1-4684-5409-3_2.
31. Allen, J. E., Gardner, S. N. & Slezak, T. R. DNA signatures for detecting genetic engineering in bacteria. *Genome Biol.* **9**, R56 (2008).
32. Greiner, R., Konietzny, U. & Jany, K. D. Is there any possibility of detecting the use of genetic engineering in processed foods? *Z. f. ür. Ernährungswissenschaft* **36**, 155–160 (1997).
33. Konietzny, U. & Greiner, R. Model systems for developing detection methods for foods deriving from genetic engineering. *J. Food Composition Anal.* **10**, 28–35 (1997).
34. Mueller, S. On DNA signatures, their dual-use potential for GMO counterfeiting, and a cyber-based security solution. *Front. Bioeng. Biotechnol.* **7**, 189 (2019).
35. Liang, C., Wagstaff, J., Aharony, N., Schmit, V. & Manheim, D. Managing the transition to widespread metagenomic monitoring: Policy considerations for future biosurveillance. *Health Security* **21**, 34–45 (2023).
36. FELIX. https://www.iarpa.gov/research-programs/felix (2017).
37. Mullin, E. How to detect a man-made biothreat. Wired, https://www.wired.com/story/how-to-detect-a-man-made-biothreat/ (2022).
38. van der Helm, E., Genee, H. J. & Sommer, M. O. A. The evolving interface between synthetic biology and functional metagenomics. *Nat. Chem. Biol.* **14**, 752–759 (2018).
39. Karlsson, O. E. et al. Metagenomic detection methods in biopreparedness outbreak scenarios. *Biosecurity Bioterrorism Biodefense Strat. Pract. Sci.* **11**, S146–S157 (2013).
40. Pasin, F., Menzel, W. & Daròs, J. Harnessed viruses in the age of metagenomics and synthetic biology: an update on infectious clone assembly and biotechnologies of plant viruses. *Plant Biotechnol. J.* **17**, 1010–1026 (2019).
41. Frey, K. G. & Bishop-Lilly, K. A. Chapter 15 - next-generation sequencing for pathogen detection and identification. In Sails, A. &

Tang, Y.-W. (eds.) *Methods in Microbiology*, vol. 42 of *Current and Emerging Technologies for the Diagnosis of Microbial Infections*, pp. 525–554 (Academic Press, 2015). https://www.sciencedirect.com/science/article/pii/S0580951715000136.
42. Israeli, O. et al. Rapid identification of unknown pathogens in environmental samples using a high-throughput sequencing-based approach. *Heliyon* **5**, e01793 (2019).
43. Li, N. et al. High-throughput metagenomics for identification of pathogens in the clinical settings. *Small Methods* **5**, 2000792 (2021).
44. Kaufman, J. Detecting genetically engineered viruses with metagenomic sequencing. https://naobservatory.org/blog/detecting-genetically-engineered-viruses (2024).
45. Ko, K. K. K., Chng, K. R. & Nagarajan, N. Metagenomics-enabled microbial surveillance. *Nat. Microbiol.* **7**, 486–496 (2022).
46. Gargis, A. S., Cherney, B., Conley, A. B., McLaughlin, H. P. & Sue, D. Rapid detection of genetic engineering, structural variation, and antimicrobial resistance markers in bacterial biothreat pathogens by nanopore sequencing. *Sci. Rep.* **9**, 13501 (2019).
47. Gilchrist, C. A., Turner, S. D., Riley, M. F., Petri, W. A. & Hewlett, E. L. Whole-genome sequencing in outbreak analysis. *Clin. Microbiol. Rev.* **28**, 541–563 (2015).
48. Fogel, G. B. et al. Identification of synthetic engineering in prokaryotic genomes using evolved neural networks. In *2022 IEEE Conference on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB)*, pp. 1–8. https://ieeexplore.ieee.org/abstract/document/9863024 (2022).
49. Collins, J. H. et al. Engineered yeast genomes accurately assembled from pure and mixed samples. *Nat. Commun.* **12**, 1485 (2021).
50. Adler, A. et al. Ensemble detection of dna engineering signatures. *ACS Synth. Biol.* **13**, 1105–1115 (2024). This paper presents GUARDIAN, a computational pipeline highlighted as an excellent example of best practices in biosecurity tool development and a key recent advance in the detection problem.
51. Roehner, N., Mante, J., Myers, C. J. & Beal, J. Synthetic biology curation tools (SYNBICT). *ACS Synth. Biol.* **10**, 3200–3204 (2021).
52. Wishart, D. S. et al. PlasMapper 3.0—a web server for generating, editing, annotating and visualizing publication quality plasmid maps. *Nucleic Acids Res.* **51**, W459–W467 (2023).
53. McGuffie, M. J. & Barrick, J. E. pLannotate: engineered plasmid annotation. *Nucleic Acids Res.* **49**, W516–W522 (2021).
54. Gretton, D. et al. Random adversarial threshold search enables automated dna screening (2024). https://doi.org/10.1101/2024.03.20.585782 (2024).
55. Jeffery, C. J. Current successes and remaining challenges in protein function prediction. *Front. Bioinformatics*, **3**. https://doi.org/10.3389/fbinf.2023.1222182 (2023).
56. Baker, D. & Church, G. Protein design meets biosecurity. *Science* **383**, 349–349 (2024). This article is written by David Baker, the PI behind RFDiffusion and 2024 Nobel Prize Winner, in conjuction with another leading synthetic biologist George Church, proposing possible regulatory mechanisms on protein design.
57. Gligorijević, V. et al. Structure-based protein function prediction using graph convolutional networks. *Nat. Commun.* **12**, 3168 (2021).
58. Kulmanov, M. & Hoehndorf, R. DeepGOPlus: improved protein function prediction from sequence. *Bioinformatics* **36**, 422–429 (2019).
59. Olson, E. J., Hartsough, L. A., Landry, B. P., Shroff, R. & Tabor, J. J. Characterizing bacterial gene circuit dynamics with optically programmed gene expression signals. *Nat. Methods* **11**, 449–455 (2014).
60. Siegal-Gaskins, D., Tuza, Z. A., Kim, J., Noireaux, V. & Murray, R. M. Gene circuit performance characterization and resource usage in a cell-free "breadboard". *ACS Synth. Biol.* **3**, 416–425 (2014).
61. Gibson, D. G. et al. Enzymatic assembly of DNA molecules up to several hundred kilobases. *Nat. Methods* **6**, 343–345 (2009).
62. Hu, J. H. et al. Evolved cas9 variants with broad PAM compatibility and high DNA specificity. *Nature* **556**, 57–63 (2018).
63. Nielsen, A. A. K. & Voigt, C. A. Deep learning to predict the lab-of-origin of engineered DNA. *Nat. Commun.* **9**, 3135 (2018). This paper is the primary landmark paper in the field of lab-of-origin prediction, a key area of study under the attribution umbrella.
64. Alley, E. C. et al. A machine learning toolkit for genetic engineering attribution to facilitate biosecurity. *Nat. Commun.* **11**, 6293 (2020).
65. Soares, I. M., Camargo, F. H. F., Marques, A. & Crook, O. M. Improving lab-of-origin prediction of genetically engineered plasmids via deep metric learning. *Nat. Computational Sci.* **2**, 253–264 (2022).
66. Wang, Q., Kille, B., Liu, T. R., Elworth, R. A. L. & Treangen, T. J. PlasmidHawk improves lab of origin prediction of engineered plasmids using sequence alignment. *Nat. Commun.* **12**, 1167 (2021).
67. Lewis, G. et al. The biosecurity benefits of genetic engineering attribution. *Nat. Commun.* **11**, 6294 (2020).
68. Higgins, J. J., Weaver, P., Fitch, J. P., Johnson, B. & Pearl, R. M. Implementation of a personnel reliability program as a facilitator of biosafety and biosecurity culture in bsl-3 and bsl-4 laboratories. *Biosecurity Bioterrorism Biodefense Strat. Pract. Sci.* **11**, 130–137 (2013).
69. Shiu, H. J., Ng, K. L., Fang, J. F., Lee, R. C. T. & Huang, C. H. Data hiding methods based upon DNA sequences. *Inf. Sci.* **180**, 2196–2208 (2010).
70. Gallegos, J. E., Kar, D. M., Ray, I., Ray, I. & Peccoud, J. Securing the exchange of synthetic genetic constructs using digital signatures. *ACS Synth. Biol.* **9**, 2656–2664 (2020).
71. Titus, A. J. et al. SIG-DB: Leveraging homomorphic encryption to securely interrogate privately held genomic databases. *PLOS Computational Biol.* **14**, e1006454 (2018).
72. Baum, C. et al. A system capable of verifiably and privately screening global dna synthesis. https://arxiv.org/abs/2403.14023. (2024). **This paper, a preprint at time of writing and citation, presents a key next step in a holistic system for reliable attribution coupled with advanced screening capabilities with consideration for an adversary attempting to dodge standard screening methods**.
73. Beal, J., Adler, A. & Yaman, F. Managing bioengineering complexity with AI techniques. *Biosystems* **148**, 40–46 (2016).
74. Faulon, J.-L. & Faure, L. In silico, in vitro, and in vivo machine learning in synthetic biology and metabolic engineering. *Curr. Opin. Chem. Biol.* **65**, 85–92 (2021).
75. Lawson, C. E. et al. Machine learning for metabolic engineering: A review. *Metab. Eng.* **63**, 34–60 (2021).
76. Radivojević, T., Costello, Z., Workman, K. & Garcia Martin, H. A machine learning automated recommendation tool for synthetic biology. *Nat. Commun.* **11**, 4879 (2020).
77. BIO, N. The convergence of artificial intelligence and the life sciences: Safeguarding technology, rethinking governance, and preventing catastrophe. https://www.nti.org/wp-content/uploads/2023/10/NTIBIO_AI_FINAL.pdf (2023).
78. Volk, M. J. et al. Biosystems design by machine learning. *ACS Synth. Biol.* **9**, 1514–1533 (2020).
79. Walters, W. H. The effectiveness of software designed to detect AI-generated writing: A comparison of 16 AI text detectors. *Open Inf. Sci.* **7**, 20220158 (2023).
80. Waite, D. W. et al. Development and validation of a bioinformatic workflow for the rapid detection of viruses in biosecurity. *Viruses* **14**, 2163 (2022).
81. Woods, N. D. Interstate competition and environmental regulation: A test of the race-to-the-bottom thesis*. *Soc. Sci. Q.* **87**, 174–189 (2006).

Acknowledgements

We thank all members of the Genetic Logic Lab at the University of Colorado Boulder for their comments on this work. This work was

supported by funding from the Charles Stark Draper Laboratory under the Draper Scholar Program.

Author contributions

W.M. conceptualized this work, collected references of interest, created the figures, and primarily wrote the manuscript. C.V. and C.M. provided advice on the structure and goals of the manuscript and figures, and additionally contributed to writing and editing.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to Chris J. Myers.

Peer review information *Nature Communications* thanks Peter Samuely, Brian Skinner and the other, anonymous, reviewer(s) for their contribution to the peer review of this work. A peer review file is available.