Chapter 8

Synthetic Biology Brings New Challenges to Managing Biosecurity and Biosafety

Andrew Jin and Igor Linkov

Novel biology technologies like gene editing and genetic engineering are creating a proliferation of breakthroughs in engineered biological systems that will change our world in areas ranging from medicine, to textiles, to energy. New developments in gene editing technologies, especially CRISPR-Cas9, have shown early signs of extraordinary potential in a variety of fields, including from basic research, applied biotechnology, and biomedical research. While the possibility of directly targeting and modifying genomic sequences in almost all eukaryotic cells could significantly improve standards of living, these technologies have the potential to pose serious biological hazards.

These potential threats have traditionally been categorized into biosafety and biosecurity concerns (Bakanidze et al. 2010). Biosafety mainly relates to the damaging effects from a biological agent that unintentionally impacts workers and the environment. On the other hand, biosecurity risks refer to the potential misuses of synthetic biology, such as bioterrorism, biowarfare or bioattacks that could derive from the genetic engineering of organisms. Because both biosafety and biosecurity share many of the same mechanisms for adverse outcomes, we must consider them concurrently. For example, a laboratory worker who was infected by a harmful virus may spread the virus in a similar mechanism as a lab worker who intentionally released a virus. Biosecurity and biosafety concerns about both the intentional and unintentional release of harmful biological agents is not a new phenomenon, but the growth of synthetic biology as a less expensive and more accessible field has dramatically changed the potential risks of synthetic biology.

The existing risk management frameworks for biological hazards were originally developed for different biosafety and biosecurity considerations, prior to the recent acceleration of developments in synthetic biology (Trump 2017). The development

A. Jin · I. Linkov (✉)

US Army Engineer Research and Development Center, Vicksburg, MI, USA

e-mail: Linkov@usace.army.mil

© The Author(s) 2021

B. D. Trump et al. (eds.), *Emerging Threats of Synthetic Biology and Biotechnology*, NATO Science for Peace and Security Series C: Environmental Security, https://doi.org/10.1007/978-94-024-2086-9_8

117

of biological technologies currently leaves us unprepared and vulnerable in the face of synthetic biology's potentially negative environmental consequences. Strategies of risk assessment and resilience, or the ability to prevent and to detect and recover from harmful releases of genetically engineered organisms before they permanently alter the environment, must now be developed for robust twenty-first Century biosafety and biosecurity.

The existing risk-based management strategy applied to chemical, biological, radiological, nuclear, and explosive hazards (CBRNE) is to either (a) manage threat (i.e., prevent the spread of such materials or eliminate the capacity to produce them through nonproliferation activities) or (b) reduce system vulnerability (i.e., fostering resources and protocols that harden infrastructural and social capacity to minimize the impact of such threats should they occur). Historically, these actions, derived from foundational principles of risk assessment, worked well in situations where the manipulation, use, and consequences of the hazardous materials were reasonably detectable and measurable. Further, CBRNE security principles focus more on hazardous substances that (a) are capable of development by a limited subset of actors, and (b) could be contained within a specific physical area upon release. Security policy against such hazardous substances has been one of prevention, where malicious actors are deprived of the knowledge and tools to foster harmful outcomes while others were prevented from incurring harmful accidents in their work. Given concerns of nuclear and chemical weapons as the dominating focus of CBRNE discussion, such principles were sensible for their time.

However, CBRNE strategies emphasizing the role of prevention and nonproliferation are insufficient in protecting against modern biological hazards for three main reasons. First, security threats stemming from synthetic biology are fundamentally different from those posed by chemicals, explosive, or radioactive material. For example, in the increasingly globalized and diversified field of synthetic biology, actors can use genetic engineering and editing technologies to alter or create a variety of platforms, including viruses, microorganisms, multicellular organisms, prions, and even cell-free systems (Gronvall 2019). In such circumstances, the threat in question is the engineered platform, not the passive propagation of materials through the environment. Engineered biological systems have the capability to persist, multiply, spread, and mutate beyond experimental and/or intended environmental deployment bounds, making it difficult to keep such systems under control or from interfering with the natural environment. Nuclear and chemical weapons are physically contained to the location of their use but engineered biological weapons could sweep across entire continents.

Second, exposure and vulnerability to synthetic biology threats are difficult, if not impossible, to quantify at present. We cannot confidently predict which platform might be used to generate a biological threat or weapon. Likewise, we cannot know what the target of a biological attack will be, whether it be humans, important crops, livestock, native species, the environment, or other assets. Third, it is hard to predict the consequences of release as we do not know how the weapon will be deployed

against the target. The new ability to modify almost all eukaryotic cells means that any biological system could be a mechanism of disruption for such a weapon. As discussed in related literature, strategies of disruption could range from releasing an aerosolized spray containing the pathogen into the center of mass transport, to lacing the feed of cattle, to sending a computer virus encoded in genetic material to a classified laboratory in order to hack into computers upon sequencing. Even if we were able to implement systems to capture all exposures and vulnerabilities of a biological attack on a specific system, the increasingly interconnected social, technical, and economic networks with which novel biotechnologies will interact further makes risk analysis of many individual components cost and time prohibitive.

To remain in-step with the shifting biosecurity landscape, systemic capabilities for biosecurity governance must incorporate elements of resilience alongside existing tools of prevention and nonproliferation. In contrast to risk-based approaches, resilience-based approaches acknowledge that, given the broad uncertainty of the threat landscape in biotechnology, threat events are difficult to predict but inevitably will occur in some form. Figure 8.1 highlights the key differences between the traditional risk-based method and a resilience-based strategy. Unlike risk-based strategies, resilience tracks both the impact of an attack as well as the system's ability to recover.

Fig. 8.1 Traditional (risk-based) and recovery-oriented (resilience-based) strategies system response. Risk-based approaches help prevent and mitigate the release of biothreats, while resilience-based strategies improve system recovery (Trump et al. 2020c)

8.1 Resilience as a Complimentary Philosophical Framework to Managing Potential Biohazards

Government officials and risk assessors are already grappling with the challenge of characterizing synthetic biology's hazards and identifying countermeasures to mitigate possible harms. This is against a backdrop of an explosion of activity in the synthetic biology landscape and increasingly inexpensive and widely available tools and techniques available to execute synthetic biology. This explosion is co-occurring with increasingly complex and interconnected global systems of infrastructure where new biological technologies will interact with systems across sectors, including the healthcare, agriculture, and energy sectors. The potential for an actor to engineer biological threats, either intentionally or unintentionally, is a real and present threat. A lack of a robust risk assessment and recovery strategy adds a further dimension of concern that may be impossible to ameliorate using existing safety and security operating paradigms (Greer and Trump 2019).

A 2012 National Academy of Sciences (NAS) report on "disaster resilience" defines resilience as the ability of a system to perform four functions with respect to adverse events: (1) planning and preparation, (2) absorption, (3) recovery, and (4) adaptation. While this definition has largely dominated resilience literature, this definition may conflate risk and resilience, which are two fundamentally different concepts. In this definition, adapt and recover are resilience concepts, while withstand and respond are concepts related to risk assessment; as such, risk is clearly added as a component of the definition of resilience. While risk assessment quantifies the likelihood and consequences of an event to identify critical vulnerabilities of a system and to harden vulnerable components of a system to avoid losses, resilience-based methods adopt a "threat agnostic" viewpoint. Thus, resilience is defined regardless of which specific threat hits the system. This is especially important for synthetic biology where new threats vary in type (e.g. virus, bacterium, protozoan), source (e.g. agricultural, pharmaceutical, bioweapon, etc), and adverse implications (e.g. environmental destruction, tainted agricultural products, adverse health impact, etc.). By developing threat agnostic resilience capabilities, resilient systems can absorb and recover from biosecurity and biosafety threats quickly, regardless of the specific nature of the threat.

Resilience is a philosophy as much as a methodological practice. Resilience emphasizes the role of recovery post-disruption as much as absorption of a threat and its consequences. Resilience is grounded upon ensuring system survival, as well as a general acceptance that it is virtually impossible to prevent or mitigate all categories of risk simultaneously, and before they occur. Methodologically, resilience practitioners seek to optimize limited financial and labor resources to prepare their system against a wide variety of threats—all the while acknowledging that, at some point in the future and regardless of how well the system plans for such threats, disruption will occur. The more conventional practice of risk assessment and management is concerned with accounting for systemic threats, typically undertaken on a threat-by-threat basis in order to derive a precise quantitative understanding of

how a given threat exploits a system's vulnerabilities and generates harmful consequences. Resilience complements traditional risk-based approaches by reviewing how systems perform and function in a variety of scenarios, agnostic of any specific threat.

Thus, resilience is not a substitute for principled system design or risk management. Both system design and risk management will be integral to preventing the spread of harmful biological agents into the environment, which will be key in minimizing biosecurity and biosafety risks of synthetic biology. Resilience is a complementary attribute that uses strategies of adaptation and mitigation to improve traditional risk management. Strategies to build resilience can take the form of flexible response, distributed decision making, modularity, redundancy, ensuring the independence of component interactions or a combination of adaptive strategies to minimize the loss of functionality and to increase the rate of the recovery. To address these biosecurity and biosafety challenges, risk analysis should be used where possible to help prepare for and prevent consequences of foreseeable events, but resilience must be built into systems to help them quickly recover and adapt when adverse events inevitably occur.

8.2 COVID-19 Pandemic as a Call to Action for Resilience in Biosafety and Biosecurity

On March 11, 2020, the World Health Organization officially declared the coronavirus disease 2019 (COVID-19) a global pandemic. COVID-19, an infectious disease caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), is a clear indicator that we are unprepared for the potential widespread impacts of a biological hazard. The growing complexity and interdependence within various systems, such as transportation, public health, and economic systems, have made them susceptible to widespread, irreversible, and cascading failures. COVID-19 as a biological threat has shown potential catastrophic impacts of lack of resilience.

The COVID-19 pandemic is a key example where traditional risk analysis failed to accurately quantify the potential impact of a biohazard. While the possibility of a global pandemic has been a consistent concern for risk practitioners, the specific nature of the COVID-19 threat (e.g. physical symptoms, origins, rate of transmission) were likely not as predictable. Furthermore, the probability of a global pandemic occurring was not something that was cognizant on the minds of risk managers of the diverse sectors that COVID-19 would subsequently impact such as energy infrastructure, agricultural systems, or transportation. It is in such cases that developing resilient systems which can recover quickly from shocks, regardless of their sources of failure, is paramount to reducing the impact of a hazard.

Before the COVID-19 crisis, supply chains of goods and services emphasized and defined success through the efficiency in the operation, management, and outcomes of various economic and social systems, largely driven by the incentives of

individual components. The COVID-19 pandemic revealed the importance of resilience within these highly complex, nested, and interconnected systems that deliver goods and services. Resilience is foundational for systems to absorb and manage shocks and prevent failures from cascading from one system component to another. (Hynes et al. 2020) For example, lack of resilience in medical supply chains to provide both preventative and diagnostic tools likely exacerbated the pandemic, causing failures to cascade into other sectors such as the food supply system (Dyal et al. 2020) and education (Viner et al. 2020). These failures elucidate the fact that mitigating hazards of a specific biotechnology, such as CRISPR-Cas9, on a specific sector requires cross-sectoral resilience to quickly respond to and absorb the adverse effects of failures before they cascade. Resilience requires an intersectoral perspective to understand key interdependencies between systems to enable them to quickly recover from adverse events and prevent cascading failures.

Given the high uncertainty and inability to fully predict or even characterize the wide universe of shocks and stresses that may challenge a given system over time, we argue that a systems theory serves as a beneficial resilience framework as it helps focus upon a given system functionality, agnostic of any given shock or stress. In other words, a systems-level approach to evaluating and enhancing resilience seeks to look internally at the structure and interrelationships of systems to review how impact or change to one node of a system generates cascading effects, in various degrees, to other directly and indirectly connected nodes. Within the next section, we explore how a resilience-based framework to adapting from the COVID-19 pandemic can benefit our understanding of biosecurity and biosafety, as these adverse events similarly entail biologically-grounded threats and uncertainties that entail implications for society at large.

8.3 A Domain-Based Resilience Framework to Adapt to Biosecurity and Biosafety

Linkov et al. (2013) assert that the Network-Centric Warfare (NCW) doctrine can be used to organize the key domains of components in a resilient system in conjunction with the four stages of the event management cycle defined by the NAS: (i) (prepare/plan, (ii) absorb, (iii) recover, (iv) adapt (Linkov et al. 2013). The NCW doctrine identifies four domains that create shared situational awareness and inform decentralized decision-making as follows:

1. Physical: sensors, facilities, equipment, system states, and capabilities
2. Information: creation, manipulation, and storage of data
3. Cognitive: understanding, mental models, preconceptions, biases, and values
4. Social: interaction, collaboration and self-synchronization between individuals and entities

All four of these are key to biosecurity in the future. By understanding resilience recourses throughout these domains, we consider the wide breadth of characteristics and decision inputs that may factor into system performance. Each domain is influenced in a different yet equally important manner when a critical or disruptive event arises, and success in one domain may not guarantee the same outcome another area. Without resilience all four components of these systems, a system cannot be resilient.

8.3.1 *Physical Domain*

The physical domain represents where the event and responses occur across the environment and is typically the most obviously compromised system in the midst and aftermath of an external shock or critical risk event. Physical elements can be represented by a portfolio of resilient engineering and design options that limit the exposure and damages given a biological threat. These engineering and design options include longstanding approaches of physical barriers and chemical remediation to emerging solutions related to biological engineering. They also include the development of economically feasible tools and techniques for the passive and active detection of biosecurity threats that must be developed, as early detection is an essential component in a resilience-based biosecurity policy.

While synthetic biology introduces new threats to biosafety and biosecurity, it is also an enabling technology to solutions that allow the engineering of components of biosystems that are resilient to failure. For example, Chan et al. (2016) described two microbial kill switches as “engineered safe-guard systems” to give synthetic biologists the ability to couple cell survival with a specific input signal, or to require complex environmental inputs to control circuit function (Chan et al. 2016).

The physical domain also consists of infrastructural characteristics ranging from transportation (e.g., roads, highways, railways, airports) to healthcare networks that deliver services to the public and support private business activities. As such, the physical domain of resilience thinking generally includes those infrastructural factors that are most directly impacted by a hazardous event, where the other domains include outcomes and actions that are a response to damage to physical capabilities and assets. In the physical domain, the objective of resilience analysis is to bring the infrastructural or systems asset back to full efficiency and functionality for use by its original owner or user. Recent events have shown how insufficient reserves or reliance on the global supply chain of medical supplies can make individual countries less resilient to potential biohazards when they rely on imported personal protective equipment and medical supplies (Ranney et al. 2020).

8.3.2 *Information Domain*

The information domain is where knowledge and data exist, change, and are shared. The field of synthetic biology has used open-sourcing platforms as a critical component to aid in new technology development. While these open-data resources allow for the quick dissemination of information regarding different biological systems, they also create opportunities for the dual use research of concern (DURC), in which scientific research can be used for either beneficial or malevolent purposes. In 2001, a group of Australian researchers engineered a strain of the mousepox virus, obtaining a new and more lethal strain which contributed to the understanding of poxviruses. However, this new strain could be used to engineer strains of the poxvirus that were far more lethal and transmissible for humans. (Gómez-Tatay and Hernández-Andreu 2019).

Similarly, the open-sourcing of biotechnologies opens up a wide range of concerns with “do-it-yourself” (DIY) synthetic biology. Biotechnology is becoming increasingly accessible to a larger number of people. This is especially true for synthetic biology, which aims to simplify genetic procedures and enable access to science for students. Such accessibility is exemplified by the international Genetically Engineered Machine (iGEM) competition for students and by practicing synthetic biology techniques and methods by non-professionals (DIYbio). It is unlikely that regulatory devices such as professional codes, export controls, or classification will be effective in the context of a deskilled, de-professionalized community of practitioners, nor is it likely that such regulatory devices could even cover the wide range of use cases for synthetic biology (Evans 2015).

One potential solution could be to expand information system responses in biosecurity and biosafety by learning from other DURC concerns, such as in cybersecurity. Within cybersecurity, a market has developed for the production and distribution of software exploits, with buyers sometimes paying over USD 100,000 for exploits and software vendors offering bounties for the disclosure of underlying vulnerabilities. This practice that is generating a transnational debate about control and regulation of cyber capabilities, the role of secrecy and disclosure in cybersecurity, and the ethics of exploited production and use (Kuehn and Mueller 2014).

Informational resilience during adverse events also requires quickly assembling knowledge about the threat and its recovery. However, key challenges exist in how to manage the release of data with concerns about privacy and data secrecy. For example, throughout the COVID-19 pandemic agencies have had to carefully consider questions about how to prevent reidentification of anonymized health data while balancing the need to disseminate data for researchers to improve understanding of the pandemic (Piller 2020). Big data collection and use has recently emphasized the particularization of data more so than the aggregation and generalization of data, and key questions have mounted concerning the legality, data quality, disparate data meanings, and process quality (Wigan and Clarke 2013). While the use of digitally available data and algorithms for prediction and surveillance of a potential biohazard (e.g. using cell-phone data to identifying people who have traveled to

areas where the hazard has spread or tracing and isolating the contacts of effected people) will be paramount importance in the fight against the COVID-19 pandemic, it is equally important to use these data and algorithms in a responsible manner, in compliance with data-protection regulations and with due respect for privacy and confidentiality (Ienca and Vayena 2020). A key need for synthetic biology practitioners will be to manage the level of data particularization and dissemination.

8.3.3 *Cognitive Domain*

The cognitive domain refers to the frameworks that utilize the information and physical domains to make decisions and includes perceptions, beliefs, values, and levels of awareness, which inform decision-making. Along with the social domain, the cognitive domain is the “locus of meaning, where people make sense of the data accessed from the information domain” (Linkov et al. 2013). Such factors are easy to overlook or dismiss due to a reliance upon physical infrastructure and communication systems to organize the public in response to a disaster. However, perceptions, values, and the level of awareness of the public regarding the strategies to overcome shocks and stresses are essential to the successful implementation of resilience operations. In other words, without clear, transparent, and sensible policy recommendations that acknowledge established beliefs, values, and perceptions, even the best-laid plans of resilience will fall to disrepair. A robust accounting for the cognitive domain is particularly important for instances where policymakers and risk managers may have a disconnect with the local population, such as with international infrastructure development projects of health-based interventions.

A key need to resilience in synthetic biology is developing the appropriate operating procedures, scientific methods and tools, and analytical capabilities must be readily available to quickly identify, recover from, and remediate the release of a harmful engineered biological system (Kelle 2013). Rapid diagnostic tools are needed after a threat has been detected to absorb the threat. These diagnostic tools and approaches must be able to determine (a) the type and purpose of the genetic modification made, (b) who made the modification and where, and (c) what technology or techniques were used to accomplish the modification. The clarity provided through the answers to the above questions will allow stakeholders and decision makers to better understand the present threat and prevent similar future threats. Proposed policy strategies address some of these questions, but capabilities are still lacking.

8.3.4 *Social Domain*

The social domain represents interactions between and within entities involved. This includes the organization structure and communication for making cognitive decisions. Within the context of synthetic biology, this domain contains key stakeholders throughout academia, industry, and regulatory domains. It also consists of the international organizations and governments which guide synthetic biology to maturity.

Within the field of synthetic biology, many individuals and organizations are actively tackling the biosecurity challenge. Many established synthetic biology organizations, such as the iGEM synthetic biology competition, mandate that organizational leaders and judges conduct rigorous reviews of the materials and planned experiments of each team with any concerns screened for potential hazards by a commercial partner; all of this is part of the competition's guidance for participating students (Millett et al. 2019).

Another potential solution for stakeholder engagement for resilience assessment is the Responsible Research and Innovation (RRI) approach to assess societal implications of emerging research to better align processes and expected outcomes with the needs and values of society. Where top-down governance proves insufficient, other actors such as universities, non-profits, and companies will need to act as gatekeepers and watchdogs to protect against nefarious actors. Top-down governance may then support such initiatives, which will require harmonization and communication at the international level.

Within the context of adverse event response, resilience will require largescale national and international cooperation. In the context of the global COVID-19 pandemic, countries that had improved intragovernmental coordination due to past experiences with pandemic response such as 2002–03 in Hong Kong and Singapore, and the H5N1 avian influenza in 1997 in Hong Kong, were able to quickly develop plans to sustain routine health-care service, open lines of international coordination, and train staff to adhere to new prevention and control measures (Legido-Quigley et al. 2020).

The social domain also provides an area to which careful attention should be paid in overall community resilience. Social aspects of society have impacts on physical health (Ebi and Semenza 2008). Throughout both the HIV epidemic and the COVID-19 pandemic, both governmental denialism and unsubstantiated regarding home remedies that could cure or prevent illness strongly influenced adverse outcomes (Mian and Khan 2020; Linkov et al. 2021). Even with strong public health leadership, other events, such as the democratic protests in Hong Kong, can erode the public trust of authority figures. (Legido-Quigley et al. 2020).

8.4 Discussion

The domain framework outlined here ensures policymakers and risk managers acquire a holistic understanding of how a shock or stress could trigger consequences that were previously difficult to comprehend. These domains overlap highly and work together in a system. While much of the focus on synthetic biology has been on the development of biocontainment through engineering organisms, (Lee et al. 2018; Chan et al. 2016) these developments are just one portion of the physical domain that consists encompasses the larger ecosystem of biotechnologies.

Emerging technologies, like synthetic biology, often develop out of sight of social scientists and policy commentators because institutional incentives to advance science and technology usually do not create opportunities for inquiry and discussion between developers, risk assessors, ethicists, and policy analysts at the early stages of research (Trump et al. 2020b). However, a key component of developing biosecurity and biosafety will be the co-development of the social science tools and frameworks that can elucidate the ethics, morals, and risk to health, are often relegated to an afterthought and isolated within institutions or organizations. Biosecurity and biosafety resilience will require understanding the key stakeholders that make decisions in how we prepare for, respond to, recover from and adapt to stresses, and how those stakeholders utilize new information to make biosafety and biosecurity decisions.

Biosecurity policies and practices must be updated to accommodate the novel challenges associated with synthetic biology and acknowledge the globalized and diverse nature of its threat space (Trump et al. 2020a). However, biosecurity efforts remain mired in uncertainty about the capabilities of SB and its practitioners' motivations in the growing number of contexts in which it is applied. Two decades into the twenty-first century, governments are still imposing old rules on a new technology, an insufficient strategy to provide security in the future. Given that such threats can arise at any time across the globe, scientists and policymakers have a narrow and closing window in which to develop systems-level prevention and recovery-based resilience strategy for twenty-first Century biosecurity.

References

- Bakanidze L, Imnadze P, Perkins D (2010) Biosafety and biosecurity as essential pillars of international health security and cross-cutting elements of biological nonproliferation. BMC Public Health BioMed Central. <https://doi.org/10.1186/1471-2458-10-S1-S12>
- Chan CTY, Lee JW, Ewen Cameron D, Bashor CJ, Collins JJ (2016) 'Deadman' and 'passcode' microbial kill switches for bacterial containment. Nat Chem Biol 12(2):82–86. <https://doi.org/10.1038/nchembio.1979>
- Dyal JW, Grant MP, Broadwater K, Adam Bjork MA, Waltenburg JD, Gibbins CH et al (2020) COVID-19 among Workers in Meat and Poultry Processing Facilities — 19 states, April 2020. Morb Mortal Wkly Rep 69(18):557–561. <https://doi.org/10.15585/mmwr.mm6918e3>

- Ebi KL, Semenza JC (2008) Community-based adaptation to the health impacts of climate change. *Am J Prev Med*. Elsevier Inc. <https://doi.org/10.1016/j.amepre.2008.08.018>
- Evans NG (2015) Dual-use decision making: relational and positional issues. *Monash Bioeth Rev*. <https://doi.org/10.1007/s40592-015-0026-y>
- Gómez-Tatay L, Hernández-Andreu JM (2019) Biosafety and biosecurity in synthetic biology: a review. *Crit Rev Environ Sci Technol* 49(17):1587–1621. <https://doi.org/10.1080/10643389.2019.1579628>
- Greer SL, Trump B (2019) Regulation and regime: the comparative politics of adaptive regulation in synthetic biology. *Policy Sci* 52(4):505–524
- Gronvall GK (2019) Synthetic biology: biosecurity and biosafety implications. In: *Defense against biological attacks*. Springer International Publishing, pp 225–232. https://doi.org/10.1007/978-3-030-03053-7_11
- Hynes W, Trump B, Love P, Linkov I (2020) Bouncing forward: a resilience approach to dealing with COVID-19 and future systemic shocks. *Environ Syst Decis* 40:174–184. <https://doi.org/10.1007/s10669-020-09776-x>
- Ienca M, Vayena E (2020) On the responsible use of digital data to tackle the COVID-19 pandemic. *Nat Med*. Nature Research. <https://doi.org/10.1038/s41591-020-0832-5>
- Kelle A (2013) Beyond patchwork precaution in the dual-use governance of synthetic biology. *Sci Eng Ethics* 19(3):1121–1139. <https://doi.org/10.1007/s11948-012-9365-8>
- Kuehn A, Mueller M (2014) Shifts in the cybersecurity paradigm: zero-day exploits, discourse, and emerging institutions. In: *ACM international conference proceeding series*, 15–18-September-2014. Association for Computing Machinery, New York, pp 63–67. <https://doi.org/10.1145/2683467.2683473>
- Lee JW, Chan CTY, Slomovic S, Collins JJ (2018) Next-generation biocontainment Systems for Engineered Organisms. *Nat Chem Biol* 14(6):530–537. <https://doi.org/10.1038/s41589-018-0056-x>
- Lérido-Quigley H, Asgari N, Teo YY, Leung GM, Oshitani H, Fukuda K, Cook AR, Hsu LY, Shibuya K, Heymann D (2020) Are high-performing health systems resilient against the COVID-19 epidemic? *Lancet*. Lancet Publishing Group. [https://doi.org/10.1016/S0140-6736\(20\)30551-1](https://doi.org/10.1016/S0140-6736(20)30551-1)
- Linkov I, Keenan J, Trump BD (2021) COVID-19: systemic risk and resilience. Springer.
- Linkov I, Eisenberg DA, Bates ME, Chang D, Convertino M, Allen JH, Flynn SE, Seager TP (2013) Measurable resilience for actionable policy. *Environ Sci Technol*, September: 130903081548008. <https://doi.org/10.1021/es403443n>
- Mian A, Khan S (2020) Coronavirus: the spread of misinformation. *BMC Med*. BioMed Central Ltd. <https://doi.org/10.1186/s12916-020-01556-3>
- Millett P, Binz T, Evans SW, Kuiken T, Oye K, Palmer MJ, van der Vlugt C, Yambao K, Yu S (2019) Developing a comprehensive, adaptive, and international biosafety and biosecurity program for advanced biotechnology: the IGEM experience. *Appl Biosaf* 24(2):64–71. <https://doi.org/10.1177/1535676019838075>
- Piller C (2020) Data secrecy may cripple U.S. attempts to slow pandemic. *Science* 369(6502):356–358
- Ranney ML, Griffith V, Jha AK (2020) Critical supply shortages - the need for ventilators and personal protective equipment during the Covid-19 pandemic. *N Engl J Med*. Massachusetts Medical Society. <https://doi.org/10.1056/NEJMp2006141>
- Trump BD (2017) Synthetic biology regulation and governance: lessons from TAPIC for the United States, European Union, and Singapore. *Health Policy* 121(11):1139–1146
- Trump BD, Galatsi SE, Appleton E, Bleijs DA, Florin M-V, Gollihar JD, Alexander Hamilton R et al (2020a) Building biosecurity for synthetic biology. *Mol Syst Biol* 16(7):e9723
- Trump BD, Cummings CL, Kuzma J, Linkov I (2020b) Synthetic biology 2020: Frontiers in risk analysis and governance. Springer, Cham
- Trump BD, Keisler JM, Volk KM, Linkov I (2020c) Biosecurity demands resilience. *Environ Sci Technol* 54(8):4706–4708

- Viner RM, Russell SJ, Croker H, Packer J, Ward J, Stansfield C, Mytton O, Bonell C, Booy R (2020) School closure and management practices during coronavirus outbreaks including COVID-19: a rapid systematic review. *Lancet Child Adolesc Health*. Elsevier B.V. [https://doi.org/10.1016/S2352-4642\(20\)30095-X](https://doi.org/10.1016/S2352-4642(20)30095-X)
- Wigan MR, Clarke R (2013) Big data's big unintended consequences. *Computer* 46(6):46–53. <https://doi.org/10.1109/MC.2013.195>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.