Chapter 2
Emerging Biosecurity Threats and Responses: A Review of Published and Gray Literature

Christopher L. Cummings, Kaitlin M. Volk, Anna A. Ulanova, Do Thuy Uyen Ha Lam, and Pei Rou Ng

2.1 Introduction

The field of biotechnology has been rigorously researched and applied to many facets of everyday life. Biotechnology is defined as the process of modifying an organism or a biological system for an intended purpose. Biotechnology applications range from agricultural crop selection to pharmaceutical and genetic processes (Bauer and Gaskell 2002). The definition, however, is evolving with recent scientific advancements. Until World War II, biotechnology was primarily siloed in agricultural biology and chemical engineering. The results of this era included disease-resistant crops, pesticides, and other pest-controlling tools (Verma et al. 2011). After WWII, biotechnology began to shift domains when advanced research on human genetics and DNA started. In 1984, the Human Genome Project (HGP) was formerly proposed, which initiated the pursuit to decode the human genome by the private and academic sectors. The legacy of the project gave rise to ancillary advancements in data sharing and open-source software, and solidified the prominence of "big science;" solidifying capital-intensive large-scale private-public

C. L. Cummings (✉)
North Carolina State University, Raleigh, NC, USA

Iowa State University, Ames, IA, USA

K. M. Volk · A. A. Ulanova
US Army Corps of Engineers, Environmental Laboratory, Engineer Research and Development Center, Concord, MA, USA

D. T. U. H. Lam
Genome Institute of Singapore (GIS), Agency for Science, Technology and Research (A*STAR), Singapore, Singapore

P. R. Ng
Wee Kim Wee School of Communication and Information, Nanyang Technological University, Singapore, Singapore

© 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_2

research initiatives that were once primarily under the purview of government-funded programs (Hood and Rowen 2013). After the HGP, the biotechnology industry boomed as a result of dramatic cost reduction to DNA sequencing processes. In 2019 the industry was globally estimated to be worth $449.06 billion and is projected to increase in value (Polaris 2020).

While biotechnology is lauded for its anticipated positive impacts on society, new public health challenges are also likely given the scientific and technological advances made in areas like bioengineering and gene editing (Trump et al. 2020a). Misuse of powerful biotechnologies is of significant concern, be it purposeful or accidental. For instance, the 1979 Sverdlovsk anthrax leak occurred when soviet scientists accidentally released genetically modified microorganisms from their biological weapons facility. The incident resulted in over 100 casualties in nearby populations (Sahl et al. 2016). This case not only demonstrates tragic consequences of biotechnological misuse but also highlights purposeful negligence and gross impertinence regarding international agreements, in this case the 1972 Biological Weapons Convention (BWC). The BWC was an agreement signed by 183 countries that banned biological weapons by countries' self-regulated accord to prohibit the development, production and stockpiling of biological agents or related equipment that could realize a biological attack (UNODA 2017). Since the 1970s, threats posed by biotechnological tools have become arguably more widespread as production costs have decreased while access to processing tools have increased. Technologies such as CRISPR and RT-PCR are available in many academic and research laboratories, increasing the possibility of independent actors misusing the technology for nefarious purposes. Increased access and ease of use also correlates to a greater diversity of individuals using biotechnology tools for distinct purposes—some of which are deemed unethical or antithetical to global standards for biotechnology research and application. An infamous example is the 2018 experiment that resulted in the birth of two twin girls where a research group applied CRISPR technology to immunize the embryos against HIV. Although this isolated incident did not pose direct national security threats, the experiment does open up a "Pandora's box" of possible unethical misuses (Raposo 2019). Following this pernicious history, there is a demonstrated need for the development and synthetization of a coordinated biotechnology framework that can better prioritize and anticipate biotechnological risks while seeking to maximize the potential benefits of applications.

Biosecurity frameworks' essential function is to create a protocol that minimizes the collateral damage of pathogens and pests. The BWC is a keystone of international biosecurity policy that arose out of the need to protect nations from the threat of an engineered biological attack. The US Department of Agriculture defines biosecurity as the methods and procedures intended to "prevent the introduction, delivery, and spread of disease pathogens that can harm or adversely affect livestock, crops, environments and people," (USDA APHIS 2020). Similar to biotechnology, the principles behind biosecurity are based in agriculture and prioritize the need to protect monocultures of crops, livestock, and poultry, whose lack of genetic diversity makes them especially vulnerable to disease. As the biotechnology field progressed and new capabilities in gene sequencing, synthesis, and modification were

refined, democratized, and globalized over the past decade, advanced biotechnology practices and products required greater prioritization of biosecurity practices and considerations.

Biosecurity threats include biological weapons and accidental releases as demonstrated in the Sverdlovsk anthrax event, but they have also become more diversified and complicated as researchers develop and utilize advanced biotechnology techniques for the betterment of society across other sectors. Gene drives for mosquito population control, engineered algae for biofuel creation, and recreation of extinct pathogens for novel vaccine development have unique and potentially unknown associated risks. The envisioned coordinated biosecurity framework would allow for beneficial innovation to proliferate while simultaneously reducing anticipated and unanticipated risk of harm to humans, animals, agricultural, and the environment (Trump et al. 2020b; Wells et al. 2020).

Many experts in the fields of public policy, public health, biotechnology, and more have discussed the threats that biotechnology may pose and the appropriate biosecurity responses from their diverse perspectives. To date, there has been no synthesis of published and gray literature regarding biosecurity. This chapter fills this gap in order to advance understanding of this quickly growing field. This chapter aims to define the typology of issues related to modern biosecurity threats and responses by coalescing disparate perspectives on biosecurity into a single descriptive location. In sum, we analyzed over one hundred peer-reviewed documents from 26 countries in order to identify reported threats and responses across global sources. The most prevalent threats identified in our analysis include dual use research of concern, biological weapons, and the ecological impact of advanced biotechnology products, while the most prevalent responses include regulation and legal oversight of the biotechnology field, risk assessment and management, frequent and open communication between researchers, government, industry, and the general public, and a strong adherence to ethics in the scientific community and subsequent self-governance. These threats and responses, in addition to less frequently mentioned ones, are discussed in this chapter.

2.2 Methods

We began our analysis with a systematic review of articles, where only published peer-reviewed articles (e.g., commentary, perspective, opinion, review articles) with available full-text were included. We started the systematic review process in the summer of 2019 and only articles published in the previous five years (2014 onwards) were considered for sampling as the area of interest is a recent emerging field (Fig. 2.1). The four databases we used to identify relevant articles were PubMed, Web of Science (WOS), Scopus, and ProQuest. We selected these databases as they provide a comprehensive collection of biomedical, life sciences, and social sciences articles. As we employed PubMed to execute the search, the Medical Subject Headings (MeSH) in PubMed were also utilized to acquire highly-specific

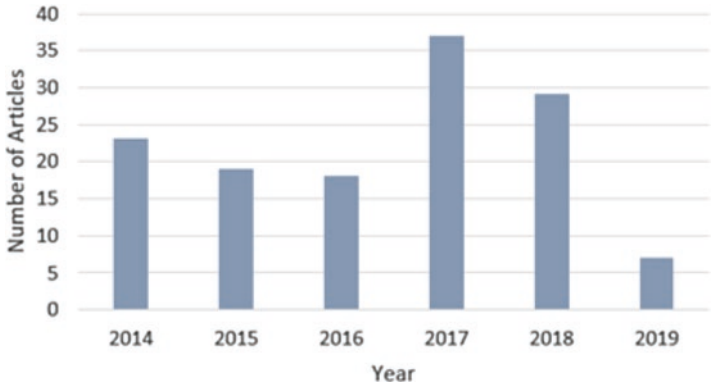

Fig. 2.1 Number of articles published between 2014 and summer of 2019 selected for our systematic review of advanced biotechnology biosecurity concerns

results based on specific medical search terms included below. The focus of our chapter is on the biosecurity threats and their proposed responses stemming from advanced biotechnology in the area of synthetic biology. Therefore, we selected search terms such that a wide range of relevant technologies were included: "gene drive", "virus", "micro", "gene edit", "CRISPR", "cell free", and "synthetic biology." To ensure thorough coverage of biosecurity issues, we employed different implicated terms. These terms included "biosecurity", "weapon", "defense", and "dual-use." We also applied different spellings (e.g. "gene edit*" and "bio-security") of the search terms to ensure that we obtained a comprehensive list of articles (Table 2.1).

First-level analysis included data "cleaning" to improve the relevance of the final sample of articles. We read each abstract provided by the databases to gauge the relevance of the article and to screen out any non-relevant results. We removed articles that addressed solely the technical aspect of advanced biotechnologies and articles that addressed other biosecurity concerns irrelevant to advanced biotechnologies. We also excluded papers with no or marginal discussion on biosecurity issues and/or measures, articles written in languages other than English, and articles in which the key words (e.g. "weapons"," defense") were used only metaphorically (Table 2.1). These criteria yielded 84 articles from PubMed (MeSH included), 119 articles from WOS, 145 articles from Scopus, and 184 articles from ProQuest. We then combined all of the articles gained from the four databases and removed any duplicates, bringing the total down to 166 articles. We were unable to obtain PDFs for 33 of these articles. Since this prevented us from analyzing the full content of these articles, we removed them from our review. The final number of articles included in our systematic review is 133.

In addition to the systematic review of peer-reviewed literature, we also sought to identify what different government agencies report about advanced biotechnologies and biosecurity and compare it with the common themes identified in the

Table 2.1 The frequency of reported articles by search term and database

Search term	PubMed	PubMed (MeSH)	WOS	Scopus	ProQuest
Biosecurity "synthetic biology"	27 **(13)**		35 **(20)**	40 **(23)**	26 **(5)**
Bio-security "synthetic biology"	0		0	2 **(2)**	1 **(0)**
Biosecurity "gene edit*"	0		6 **(4)**	7 **(7)**	67 **(7)**
Bio-security "gene edit*"	0		0	1 **(1)**	0
Weapon* "synthetic biology"	9 **(3)**		8 **(4)**	14 **(7)**	138 **(12)**
"Warfare agent*" "synthetic biology"	2 **(0)**		5 **(2)**	6 **(2)**	14 **(2)**
Defense "synthetic biology"	81 **(4)**		51 **(3)**	51 **(5)**	96 **(4)**
Weapon "gene edit*"	0		8 **(3)**	13 **(5)**	72 **(8)**
"Warfare agent*" "gene edit*"	0		3 **(3)**	3 **(3)**	7 **(1)**
Defense "gene edit*"	0		107 **(1)**	113 **(2)**	51 **(1)**
Biosecurity "dual-use"	36 **(27)**		32 **(20)**	57 **(39)**	83 **(31)**
Bio-security "dual-use"	0		0	4 **(1)**	4 **(3)**
Biosecurity "gene drive"	4 **(3)**		3 **(3)**	7 **(7)**	23 **(13)**
Bio-security "gene drive"	0		0	0	0
Biosecurity "micro*"	17 **(0)**		202 **(5)**	472 **(4)**	2625 **(26)**
Bio-security "micro*"	1 **(0)**		5 **(0)**	21 **(0)**	130 **(2)**
Biosecurity "cell-free"	2 **(0)**		1 **(0)**	1 **(0)**	44 **(1)**
Bio-security "cell-free"	0		0	0	2 **(0)**
Biosecurity "CRISPR"	22 **(8)**		10 **(9)**	11 **(8)**	103 **(27)**
Bio-security "CRISPR"	0		0	0	1 **(0)**
Biosecurity "virus"	1199 **(7)**		526 **(21)**	603 **(13)**	1707 **(39)**
Bio-security "virus"	11 **(0)**		9 **(0)**	29 **(2)**	87 **(2)**
Biosecurity "*virus"	1199 **(7)**		547 **(21)**	632 **(12)**	0
Bio-security "*virus"	11 **(0)**		9 **(0)**	30 **(2)**	0
Gene drive technology		13 **(12)**			

Non-bolded numbers give the frequency before initial screening of abstracts, while the bolded numbers in parentheses give the frequency after initial screening and abstracts
MeSH medical subject headings, *WOS* web of science

peer-reviewed literature. We focused on government documents published by the US and the EU as they dominated the academic conversation on biosecurity (Fig. 2.2). The National Academies of Sciences, Engineering, and Medicine's (2018) report *Biodefense in the Age of Synthetic Biology* was analyzed for the US and the European Commission's (2017) report *Action Plan to Enhance Preparedness against Chemical, Biological, Radiological and Nuclear Security Risks* was analyzed for the EU (Fig. 2.3).

Our next step was to analyze the content of each article. To do this, we read through each document and identified any biosecurity threats and responses (i.e.

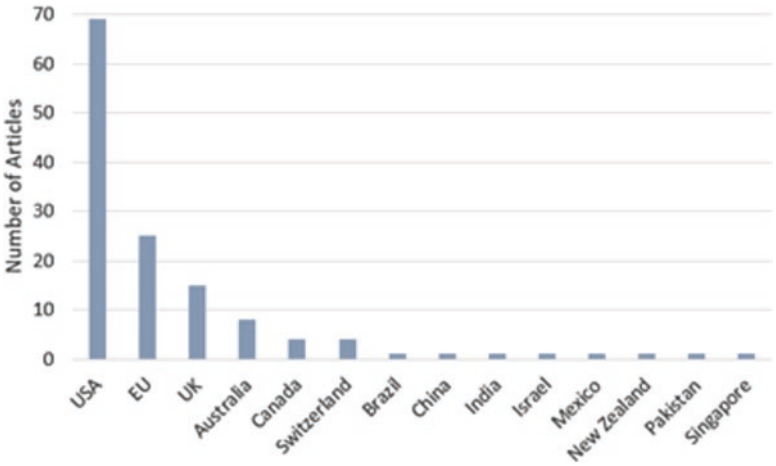

Fig. 2.2 The number of articles within the systematic literature review published from each country as determined by the affiliation of the corresponding author

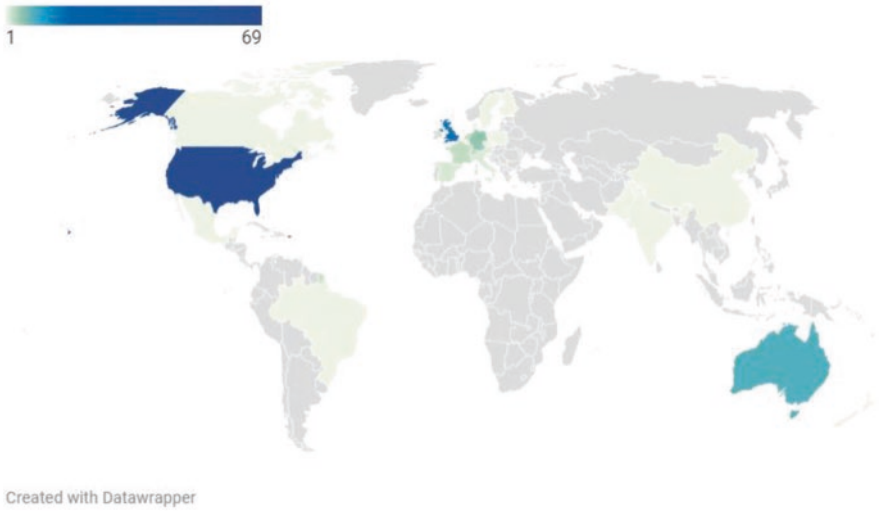

Fig. 2.3 Map displaying which countries published literature used in our systematic review and the relative frequency of publications from each country, as determined by the affiliation of the corresponding author

solutions to biosecurity threats) described in the document. We then grouped common threats and responses until we had a comprehensive and manageable list of biosecurity threats (Table 2.2) and expert-recommended responses (Table 2.3). This processes followed a grounded theory coding structure to ensure that we maintained a theoretical sampling perspective with, "the aim being to explore the dimensional

Table 2.2 Biosecurity threats and the frequency of articles reported

Biosecurity threat	Frequency	Percent of articles (%)
Dual use	66	50
Bioweapon	37	28
Ecological impact	29	22
Accidental release	26	20
Bioterrorism	23	17
Gain of function	16	12
Societal impact	16	12
Information access	12	9
Lower barriers	9	7
Uncertain consequences	7	5
DIY community	5	4
Difficult to monitor	4	3
Theft	4	3

Table 2.3 Biosecurity repsonses and the frequency of articles reported

Biosecurity response	Frequency	Percent of articles (%)
Legal oversight	59	44
Communication/open discussion	49	37
Risk assessment/management	45	34
Self-governance/ethics	37	28
Education/training/awareness	35	26
Collaboration	30	23
Biosafety principles	29	22
International governance/guidelines	25	19
Surveillance	19	14
Augment access	19	14
Improved response capacity	13	10
Containment or reversal strategies	7	5
Funding	6	5

range or varied conditions along which the properties of concepts vary" (Corbin and Strauss 1990, p. 73). Using the constant comparative method, each article was compared against one another to inductively assess potential emergent themes without *a priori* assumptions of the content or form of those themes. This inductive analysis design allows for sought-after themes to emerge from patterns present in the cases under analysis without presupposing what the important themes will be (Patton 2014). Next we report the key themes identified across our samples regarding biosecurity threats and responses.

2.3 Results and Discussion

2.3.1 US and EU Governmental Frameworks

2.3.1.1 US Framework

The process of creating a biodefense framework for the United States of America follows several engineering paradigms, with the Specify-Design-Build-Test-Learn (SDBTL) cycle being the guiding principle (NASEM 2018). In the SDBTL cycle, researchers are able to systemically identify the desired organism or the organism's functionality that will be genetically altered in a synthetic biology (SynBio) experiment. The researchers will then be able to assess the success of the alteration and amend the experimental protocol if needed. This empirical process has given fruition to a framework by the National Academy of Science, where certain parameters of biotechnology can be used to qualify a level of concern or hazard in the usability of a certain SynBio related technology. It must be noted that this framework aims not to enumerate the level of risk, but to direct concern to where the technology might be the most compromised. The concern about SynBio-related technology stems from the potential of its nefarious use, creating an objective assessment of achievements and shortcomings. The framework can be summarized into four parts: usability of technology, usability as a weapon, requirement of actors, and potential for mitigation. The four parts can be further broken down into subparts that can be assessed more easily.

Usability of Technology can be decomposed into four categories: ease of use, rate of development, barriers to use, and synergy with other technology. Ease of use is related to the commonality of the technology or of the information. The more widespread and accessible the technology is, the more accessible it is to nefarious actors, thereby increasing its threat. Rate of development refers to rapidity of improvements/innovations, whether there is a defined common use of the technology and if the technology is relevant throughout the times. For example, if a new technology does not have an intended use and there is a lot of funding behind the development of the product, the technology would generate concerns over its misuse. Barrier to use refers to the hurdles that can limit the use of technology, with hurdles being factors such as the accessibility of knowledge on how to operate the technology, the accessibility of materials needed for the technology, and other parameters. The lower the barrier of usage, the higher the concern about the technology. Synergy with other technology assesses whether there are other technologies present that can enhance the effects. Thus, the presence of synergy with other tools would increase the overall level of concern.

Usability as a Weapon is an assessment based on three other factors: production and delivery, scope of casualty, and predictability of results. Production and delivery refer to whether a genetically engineering organism, or any other product related

to biotechnology, can produce toxins or other nefarious substances that can endanger people's lives. Production and delivery can be done inadvertently or carried out with a purpose. Therefore, as the production and delivery increases, the concern increases as well. Scope of casualty refers to the scale of the potential threat. A higher scope of casualty means more people are being endangered, which increases the level of concern. The predictability of results refers to the certainty of a nefarious user getting their intended results. This can be measured in the need for testing and if phenotype predictability is present. If testing is not needed to achieve the desired effects, then the level of concern and biosecurity threat increases since there are reduced opportunity for authorities to recognize and prepare for an attack for attack. If phenotype predictability is high, then the nefarious user has some confidence that the protocol they have followed will result in success. Therefore, as the phenotype predictability increases, so does the level of concern.

Requirements of Actors is an assessment of the feasibility of perpetrators successfully using specific biotechnology to commit a planned attack. The successful completion depends on the access to enterprise, access to resources, and organizational footprint. Access to enterprise relates to whether the actors have interaction with or access to the tools of question. Access to resources refers to whether the actors have the resources to carry out their attack. Resources can include items such as money, raw ingredients, and laboratory space. Lastly, organizational footprint is an estimate on how much manpower is needed to complete the attack. The more people an organization needs to complete an attack, the lower the concern level.

Potential for Mitigation is an assessment of areas of concern that can be addressed before an attack or an event occurs. The analysis is broken into four subparts to create a holistic examination of policies or accessibility issues that can compromise biosecurity. The first part is deterrence and prevention capabilities, which identify potentially dangerous activities and take steps towards preventing these activities. Actions such as increased intelligence gathering and instituting regulatory safeguards to areas of concern are effective in preventing certain tools from wreaking havoc. The second step in assuagement is developing the capability to recognize an attack. The identification process depends heavily on public health and disease databases as well as surveillance systems. By identifying and outlining the pre-existing tools available, the identification process can be optimized. Another step in mitigating a potential threat is attributing capabilities of an attack to a certain group. In simpler terms, matching the scientific evidence left at the attack to the organizations that have done it. The more difficult it is to identify the culprit, the higher the level of concern. The last step for mitigating a potential threat is developing an appropriate response to a myriad of attacks. Consequence management capabilities refers to a series of protocols and procedures that are established before an attack happens in order to quickly and efficiently respond to the attack and minimize the damage done. The procedures often include increasing emergency response capacity, developing quarantining facilities and expanding healthcare facilities.

2.3.1.2 EU Framework

The 2017 European Union (EU) Chemical, Biological, Radiological and Nuclear (CBRN) Action Plan outlines a general framework on improving prevention, preparedness, and response in case of an attack. The document also includes a clause that obligates EU member states to provide assistance to those victims of CBRN attacks and to maintain communication between countries within and outside the EU. Although the action plan covers responses to other threats that are not biological, most of the identified threats and responses are ubiquitous in application to biosecurity. The framework can be split into four actions: reducing accessibility of materials, ensuring preparedness for incidents, building stronger links, and enhancing current knowledge of risks.

The frameworks primary concern is **limiting the accessibility of potential dual-use technology or any other hazardous materials**. Increasing the legal control of law reinforcement and preventing the trade of dangerous material to nefarious actors is one viable option. Methods of accessibility reduction include providing technical reports on weapons and incidents through Europol and strengthening patrol at EU borders. This action can increase the awareness of potential threats in law enforcement personnel and hinder the spread of material that can be used to initiate an attack. Another implementation measure that can limit the accessibility of materials is to decrease insider threats by optimizing vetting and background checks of personnel in facilities holding CBRN materials in order to identify and remove individuals with nefarious intentions.

The second step identified in the action plan is to ensure that **member states are prepared to respond to a CBRN incident**. Due to the diversity of the European Union, safety protocols get adopted at various levels of intensity depending on the economic and political status of the member state. The first proposed action towards a uniform response to CBRN incidents is to develop a common training curriculum and institute cross-sectorial training and exercise. Other measures to improve overall preparedness for potential attacks include systematic review and assessments of previous CBRN Action Plans and strengthening the current European Emergency Response Capacity of the Union Civil Protection Mechanism by registering proposed CBRN modules. Updating current technologies and systems used for monitoring CBRN materials is imperative to stay relevant to the technologies available to nefarious actors. Conducting a gap analysis on CBRN material detection and improving the Early Warning and Response System (EWRS) can be a vital strategic advantage for EU states against malignant actors. Concurrently, improving the ability for laboratories to identify CBRN material and improving medical countermeasures such as joint efforts in research and development of vaccines should be pursued. Pertaining specifically to biosecurity, it is essential to increase overall awareness and develop a response protocol for emerging bio-risks.

Building stronger internal-external links in CBRN security with key regional and international EU partners was also identified in the framework. While most of the previous content was focused on strengthening the flow of information and resources within the EU, the later part of the framework focused on maintaining a

similar level of contact with foreign entities outside of the EU. Particularly with NATO, the primary aim of the partnership is to develop a counter-terrorism protocol by increasing information exchange, capacity building, training, and exercise. This ties into the final section of the EU CBRN framework: **enhancing current knowledge on CBRN risks**. This last section focused primarily on the creation and application of a security network. The EU CBRN security network will be overseen by a dedicated advisory group, and will make information available for sharing with Europol. The maintenance of the research network will depend on updating prevalent needs and threats relating to CBRN.

2.3.2 Threats Identified in the Literature

The thirteen biosecurity threats identified in the literature are summarized in Table 2.2. On average, each article mentioned two threats (min = 0, max = 8). Each threat, as informed by the literature, is further described and discussed below.

Dual Use was the most frequently mentioned threat, appearing in half of the analyzed articles. Dual use research of concern is defined as "life sciences research that, based on current understanding, can be reasonably anticipated to provide knowledge, information, products, or technology that could be directly misapplied to pose a significant threat with broad potential consequences to public health and safety, agricultural crops and other plants, animals, the environment, material, or national security," (Lev and Samimian-Darash 2014). DiEuliis and Giordano (2018) further state that "any tool that imparts great capability also involves at least some risk, if not threat, that the power conferred by such capacity can be used to leverage or evoke a variety of ends." This is at the center of the concern over dual use research. The majority of biotechnology research and modernization is legitimate and done with the goal of benefiting society – that is, to beneficial ends. However, the same knowledge and techniques gained from beneficial research can be used maliciously. For instance, CRISPR-Cas9 is being used to perform targeted gene editing as a treatment for cancer, increasing our ability to treat cancer and reducing our reliance on toxic chemotherapy drugs, but it could also be used to edit pathogens to increase their virulence. Indeed, the dual use applications and threats from CRISPR are prominently featured in the literature (Vogel and Ouagrham-Gormley 2018; Webber et al. 2015).

Much of the controversial dual use research in biotechnology involves **gain of function** (GOF) studies, a term used in 12% of articles. Duprex et al. (2014) considers GOF to be a "generic label for a broad class of experiments that lead to a genetically altered biological agent with new or enhanced functions." Much of the concern over GOF studies includes research on the avian influenza virus and relatives of the smallpox virus (Evans et al. 2015; Duprex et al. 2014). These studies conferred new traits to the virus that increased its virulence in order to study transmission or vaccine creation, but also have a clear application for biological weapon (bioweapon)

development. In this way, they are both GOF and dual use research. Publishing these sorts of studies is considered a biosecurity threat of its own because the information could allow a nefarious actor to create a bioweapon when they otherwise wouldn't have had the knowledge to do so. We refer to this threat as "**information access**" and it is mentioned in 9% of articles. DiEuliss and Gronvall (20) touch on this threat while writing about the controversial publication of a study that synthesized horsepox from scratch. They state that "horsepox is not a significant disease for humans, but there is concern that publication of these experiments could lower barriers toward the synthesis and booting up of another orthopoxvirus, variola (smallpox) virus, which was a significant scourge in history."

Bioweapons were the second most frequently mentioned threat, appearing in 28% of the articles analyzed. Franconi et al. (2018) define bioweapons as "deadly pathogens – bacteria or viruses – or toxins that can be deliberately released in order to cause harm to people or animals and plants." Generally, when a bioweapon is used by a state sponsored entity it is considered an act of biowarfare, while the use of a bioweapon by a non-state sponsored entity or individual is considered an act of **bioterrorism** (Jamil 2015), the latter of which was mentioned in 17% of articles. Unaltered organisms can and have been used as bioweapons in the past, such as in the 2001 anthrax attacks. Biotechnology opens the door to creating enhanced or novel pathogens and new avenues for toxin production. Cross (2018) identifies three ways in which biotechnology can be used to create bioweapons: (1) "recreating pathogenic viruses such as Ebola, SARS, or smallpox," (2) "engineering bacteria to make them more dangerous, which could be easily accomplished by inserting genes to confer antibiotic resistance," and (3) "engineering microbes to produce and release toxic biochemicals." Researchers have already demonstrated capabilities in all three of these avenues. Horsepox, a close relative of smallpox, has been synthesized from mail-ordered DNA (Noyce et al. 2018), avian influenza has been engineered to allow for airborne transmission between mammals (Linster et al. 2014), and botulinum toxin has been produced using yeast cells (Fonfria et al. 2018). These three cases are also prime examples of dual use research, as they were carried out for beneficial purposes (vaccine development, study of transmission, and enhanced therapeutics, respectively) but also provide a clear avenue towards weaponization.

Bioweapons and bioterrorism are mainly concerned with the deliberate release of an engineered pathogen or toxin with the purpose of causing harm, but the literature also identified **accidental releases** of modified organisms as a threat. Accidental releases are often cited as a concern for biosafety and not biosecurity. Pastorino et al. (2017) delineates the two terms in a laboratory setting as follows:

> "Laboratory biosafety" is the term used to describe the containment principles, technologies, and practices that are implemented to prevent unintentional exposure to pathogens and toxins or their accidental release. "Laboratory biosecurity" refers to institutional and personal security measures designed to prevent the loss, theft, misuse, diversion, or intentional release of pathogens and toxins."

Legitimate research on the most dangerous pathogens are often restricted to laboratories with a high Biosafety Level (BSL) designation – as regulated/monitored by a

country's federal disease agency and the World Health Organization. These laboratories have the necessary precautions to drastically reduce the risk of inadvertently releasing wild type or engineered pathogens (Imperiale et al. 2018). Accidental releases are a higher threat if work is being done in laboratories without proper safety measures, such is in the growing biotechnology Do-It-Yourself (DIY) community. The risk of unintentional releases also increases as engineered organisms are taken outside of the laboratory setting, such as in the case of bacteria engineered for soil bioremediation or algae engineered for biofuel production and grown in outdoor open-air tanks (Mandel and Marchant 2014). In both of these cases, the engineered organisms have the potential to escape outside of the intended soil or water and have unknown consequences for the receiving environment.

Regardless of how an engineered organism or virus makes it out into the open, the potential ecological and societal impacts were frequently identified as concerns. Interestingly, concerns over ecological impacts appeared in 22% of articles, almost twice as many articles as societal impacts which appeared in 12% of articles. While bioweapons could be created to directly attack some critical component the environment, the concern over **ecological impacts** is largely driven by the increased interest in using engineered organisms for controlling nuisance species and recent advancements in gene drive technology. Weidmann (2018) defines gene drives as the "experimental techniques which are supposed to push foreign genes into the chromosomes of wild populations with the aim to change the complete organisms in just a few generations." Popular examples of the potentially beneficial application of gene drives include reducing populations of mosquitos responsible for spreading dengue fever and malaria (Finkel et al. 2019; Weidmann 2018) and exterminating introduced rodents that predate on endangered reptiles and birds from islands (Weidmann 2018). However, since biological organisms and viruses are capable of reproducing, mutating, and sharing genes, there is little way to guarantee that the intended modification will be contained in the target population only and little way to anticipate the cascading environmental consequences of manipulating populations of species in such a way. This is at the heart of the threat advanced biotechnology poses to ecological systems and is discussed in multiple papers. Weidmann considers gene drives "ethically questionable because we still do not know if the genetic changes could affect other organisms or even entire ecosystems in a negative way." Wintle et al. (2017) raises the similar concern that "deploying gene drives in wild populations might alter ecosystems, disrupting trophic levels and food webs, and creating vacant niches (for example, for new disease vector species or new disease organisms)." Webber et al. (2015) conclude that "removing species with gene drive technology could produce unintended cascades that may represent a greater net threat than that of the target species." Overall, concerns of the negative and irreversible impact that one genetically engineered species could have on the entire ecosystem was evident in the literature.

These quotes, and the inherent ability of biological systems to mutate and evolve, also demonstrate the threat of the **uncertain consequences** of utilizing and deploying advanced biotechnology, which was expressed in 5% of articles. Ecological systems are filled with complex, intricate, and unknown interactions (from the

global to the intracellular level) and advanced biotechnology is still a young and rapidly developing field with only a few examples of field trials with engineered organisms (Seager et al. 2017). When these two complex components are considered in tandem, it is not surprising to see in the literature that some experts are concerned that consequences cannot be reliably foreseen and avoided.

Threats to human health are abundant in the conversation of bioweapons and bioterrorism, in which enhanced pathogens that could cause mass human casualty are a primary fear. However, **societal impacts** as identified in this chapter are less concerned with human health and more concerned with human or environmental modification and how these alterations would impact society. Caballero-Hernandez et al. (2017) suggest that gene drives used to control nuisance species could impact a nation's food security and national sovereignty, though they do not elaborate on how. Esvelt and Gemmell (2017) also mention the problem of national sovereignty and gene drives, in that one nation risks infringing on the national sovereignty and harming diplomatic relations with another nation if they release an engineered strain of a species that is found in both nations without the other nation's consent since the engineered strain will cross national borders. Concerning human modification, genome editing has been proposed as a way to remove undesirable traits from a human population, increase the average cognitive ability of a nation, and enhance combat soldiers by decreasing the need for sleep and food (Esvelt and Millett 2017), all of which have serious equality, security, and societal implications. Gomez-Tatay et al. (2016) propose that synthetic biology could be used to "improve humans and to develop what it has been called sub-humans, a kind of humanoid organism which would serve several purposes, such as being sources of transplantable tissues and organs, experimental subjects or crash test dummies and landmine diffusers." While this vision of sub-humans shows potential in improving life and safety for modern humans, it also has clearly negative ethical and societal implications. Considering human modification, the field of biotechnology would need to make leaps and bounds forward in order for these threats to be realized, but nonetheless they are important to consider and address as biotechnology progresses and advanced engineering of humans becomes more possible.

The **lowering of barriers** to entry into the biosecurity field and the **DIY biotechnology community** were identified as threats in 7% and 4% of articles, respectively. The lowering of barriers is largely caused by the increased globalization and democratization of the field in the past decade that has greatly increased the accessibility of the field to a wider number and diversity of people. While this has driven innovation and resulted in many beneficial applications, it has also reduced the barriers that would have previously kept nefarious individuals – whether working alone or for an organized state, sub-state, or non-state group – from using biotechnology towards their own harmful ends. It has also allowed individuals in the DIY community to construct quasi-laboratories in their own homes and carry out their own experiments devoid of regulations or safety precautions. DiEuliis and Giordano (2018) highlight these threats in relation to gene editing by stating that "the relative availability of [gene editing techniques] enables increasing use by public research and do-it-yourself (i.e., biohacking) communities which could foster risk incurred

by both inadvertent misuse and/or intentional development of products that threaten public safety." Jefferson et al. (2014) share this sentiment, but extend it beyond the DIY community by expressing fears that "the 'de-skilling' of biology, combined with online access to the genomic DNA sequences of pathogenic organisms and the reduction in price for DNA synthesis, will make biology increasingly accessible to people operating outside well-equipped professional research laboratories, including people with malevolent intentions." The ease with which people are able to access information, equipment, materials, and learn techniques is therefore a growing biosecurity threat.

The final two biosecurity threats identified in the literature were the **difficulty of monitoring** and potential **theft of pathogens or equipment**, which both appeared in 3% of articles. A number of concerns fall under the category of difficult to monitor. These include the difficulty of determining which organisms/viruses and genetic modifications could be used maliciously and monitoring for them (DiEuliis and Giordano 2017), of monitoring the spread of an engineered trait beyond where it was intentionally deployed for species control (Webber et al. 2015), and of differentiating a natural outbreak from a biological attack (MacIntyre et al. 2018; Nelson et al. 2014). Regarding theft, MacIntyre et al. (2018) and Walsh (2016) both see the ability for radicalized research staff to steal pathogens from the laboratories they have access to as a biosecurity threat. Berger and Schneck (2019) and Kozminski (2015) are additionally concerned over the threat of malicious actors stealing sensitive data that is stored digitally. Kozminski (2015) cautions that "in the area of Big Data with specific applications to the life sciences, information taken could potentially be used for exploitation or extortion." This "Big Data" includes the ever-growing databases devoted to people's genetic information collected for forensic, genealogical, or research purposes.

2.3.3 Responses Identified in the Literature

The thirteen biosecurity responses identified in the literature are summarized in Table 2.3. On average, each article mentioned three threats (min = 0, max = 8). Each response, as informed by the literature, is further described and discussed below.

Legal Oversight or Regulations at the national level were the most frequently mentioned biosecurity response, appearing in just under half of the articles analyzed. However, the form and extent of that regulation varied. The US Government Policy for the Oversight of Life Sciences Dual Use Research of Concern places restrictions on certain types of experiments on certain infectious agents and toxins (Lev and Samimian-Darash 2014). De Beer and Jain (2018) suggest that regulations need to remain loose enough to allow for innovation and that outreach and monitoring can supplement such loosening in oversight. Some articles call for regulations throughout the research and development process (Gomez-Tatay and Hernandez-Andreu 2019), carefully scrutinizing the primary investigator, purpose, location,

and process, while others advocate that mainly the end product should be subject to regulation (Gronvall 2015). Regulations dictating who can purchase what genetic material and equipment, which laboratories are approved to conduct dual use synthetic biology research, and what knowledge is appropriate to disseminate in journals were also suggested in multiple articles (Gomez-Tatay and Hernandez-Andreu 2019; Pope 2017; Adam et al. 2017; Diggans and Leproust 2019; Marris et al. 2014). These regulations also fall into **augmentation of access**, which appeared in 14% of articles and could be considered a sub-category of legal oversight. The augmentation of access includes any measures that reduce a person's ability to access equipment, materials, facilities, or knowledge required to partake in synthetic biology, thereby reducing the risk of unauthorized personnel engaging in intentionally or unintentionally harmful research.

International Agreements, Guidelines, or Regulations were also suggested, though at 19% of papers this response appeared less than half as often as national regulations did. The driving thought behind some form of international governance, in addition to the national regulations discussed above, is that any accident or attack with an engineered organism is likely to have far-reaching consequences for an entire ecoregion, continent, or the world. It is therefore in the best interest of humanity for all nations to come together and agree on best practices as they relate to advanced biotechnology. The BWC, as discussed in the introduction, is a foundational international agreement in which nations agree not to create or stockpile bioweapons. Bioweapons can be easily and objectively viewed as "bad," making regulations against them relatively simple, but much of modern advanced biotechnology exists in a more complicated grey zone owing to its dual use potential and newness as a field (Greer and Trump 2019). Experts have called for new international agreements as the field of biotechnology has diversified and its related threats have expanded past just biological weapons. A prime example is the risk posed by releasing gene drives into the environment. Redford et al. (2014) emphasize that this poses a relatively new threat and that "international regulation of the development and release of modified organisms needs considerable work," and will require "wider competence on the part of diplomats and lawyers in understanding both synthetic biology and ecology." Other experts suggest that regulations on advanced biotechnology could be applied under existing international treaties and agreements, such as the Convention on Biological Diversity, Nagoya Protocol, United Nations Security Council Resolution 1540 (non-proliferation of weapons of mass destruction), and the BWC (Gronvall 2015; Stewart 2018; Ahteensuu 2017). Citing new rules or guidelines under existing agreements that nations have already agreed to is viewed as a more stream-lined method than creating entirely new treaties and agreements.

The third most frequently mentioned response is **risk assessment or management**, which appeared in 34% of the articles we analyzed. The most frequently mentioned risk assessment method was the risk-benefit analysis, in which "the risks of potential misuse (accidental or intentional) are weighed against the assumed

potential benefits of scientific innovation," (Jacobsen et al. 2014). This analysis and other risk assessment methodology can be used to determine if a proposed study should occur. If the benefits outweigh the risks and the study is given the okay, then risk management can be used to identify "how to do it safely and mitigate risks," (Imperiale and Casadevall 2018). Risk management options proposed in the literature include laboratory biosafety (Pastorino et al. 2017), containment strategies (Duprex et al. 2014), publication restrictions (Rychnovska 2016), and more. Multiple authors called for risk assessment and subsequent plans for risk mitigation be conducted during the project planning/grant application phase. Oeschger and Jenal (2018) argue that successful risk assessment and management requires the input of "the life science research community itself as proper risk evaluation and management depends on expert knowledge." Suk et al. (2014) add that risk assessment "needs to integrate the best available information from a variety of sectors, meaning that life scientists, regulators, ethicists, public health actors, and the security and intelligence communities will need to become more adept at and comfortable with exchanging information and ideas." In this quote, Suk et al. (2014) also demonstrate the benefit of **collaboration** between experts from diverse fields in reducing biosecurity threats. The usefulness of collaboration as a response was identified in 23% of articles, and was suggested as a way to improve the identification of an outbreak (MacIntyre 2015), policy design and implementation (Edwards 2014), laboratory biosafety (Trevan 2015), public outreach (Redford et al. 2014), and biological data security (Berger and Schneck 2019), in addition to risk assessment.

Three out of the five most frequently mentioned responses had less to do with government oversight and more to do with social aspects: **communication and open discussion** between scientists, government, industry, and the public (37%); a strong sense of **ethics and self-regulation** amongst scientists (28%); and proper **training of scientists and awareness of biosecurity concerns** (27%). These three social responses are also complimentary to one another. Oeschger and Jenal (2018) state that "a code of conduct intends to promote ethical principles and corresponding behavioral norms that often go beyond legal requirements." By adopting a code of conduct, scientists "raise awareness of and foster responsibility for dual use aspects of life science research within the scientific community," (Oeschger and Jenal 2018) Fear and ter Meulen (2016) further define self-regulation as a system in which "there are checks and balances within the scientific community, not [one in which] each researcher is free to decide unilaterally which procedure to follow." Self-regulation not only requires open communication between scientists, but also for scientists to have a line of communication with the public, government regulators, and other stakeholders in order to be aware of the concerns surrounding biotechnology, see how their intended research relates to those concerns, and take appropriate actions to respond. Scientists should also communicate with the public to relieve unwarranted concerns held by the public and allow scientific research to continue. Baskin (2019) emphasizes that "intentional, careful, and reassuring communications from the scientific community to the public benefit both science and the public." Baskin (2019) stresses that while self-regulation is ideal, scientists

should also receive training in the law-making process and how to engage with it so that the scientific community can "become involved throughout the rule-making process to prevent excessive restrictions that are potentially counter-productive to national biosecurity" when legal instruments are unavoidable. According to the literature, training, communication, and self-governance have great potential for addressing biosecurity threats (Engel-Glatter and Ienca 2018; Oeschger and Jenal 2018; Baskin 2019; Gomez-Tatay et al. 2016).

The use of **biosafety principles** to reduce biosecurity threats, particularly accidental releases of engineered organisms, was identified in 22% of articles. Biosafety principles include the design of laboratories with precautions appropriate to the risk-level of pathogens being studied (BSL designations, as mentioned above), "train[ing] people that work there, the implementation of regulations, and the use of robust risk-based approaches to mitigate adverse events," (Vogel et al. 2015). Fear and ter Meulen (2016) emphasize that "attention to key biosafety issues is imperative at all stages of the research endeavor from first formulating a research idea through to the publication of results." By identifying and following appropriate biosafety precautions, studies with advanced biotechnology can be conducted with the confidence that accidental releases will not occur, that the general public and local environment will not be affected, and that workers are properly protected while performing their duties. Certain biosafety principles, such as the requirements to meet different BSL classifications, are regulated by state or federal agencies, but additional requirements could be established by individual institutions.

Many of the responses we identified looked to reduce the risk of a biosecurity threat before it could occur, but it is also important to have the capacity to recognize and respond to threats once they are present. Building a nation's **capacity to respond** to a biosecurity threat, also referred to as "preparedness strategies," before the threat is present and actively engaging in **surveillance** of present or imminent biosecurity threats were identified in 10% and 14% of articles, respectively. Nelson et al. (2014) summarizes the impact that both of these responses can have: "Surveillance strategies enable early detection, which is vital for rapid and effective emergency responses whilst preparedness strategies are essential for maintaining a nation's capacity to carry out effective response and recovery processes." They go on to report three types of surveillance that Australia uses to identify unusual disease patterns that could indicate an outbreak: "passive surveillance, involving routine reporting of certain disease cases; active surveillance, involving the specific collection of data relating to a particular disease; and sentinel surveillance, where data are collected from a subpopulation to provide an indication of trends in the wider population," (Nelson et al. 2014). Surveillance of DNA sequence orders made to DNA synthesis companies to identify and terminate potentially malicious orders has been practiced and suggested for wider adoption, as has monitoring social media and the dark web for signs that a biological attack is being planned or has occurred (MacIntyre et al. 2018). Improved response capacity includes a variety of measures aimed at quickly recovering from a biological attack, thereby reducing the amount of damage that can be done. According to Nelson et al. (2014),

"preparedness strategies incorporate aspects including: planning; personnel training; monitoring and reviewing policies and programs; maintaining supply stocks; and carrying out ongoing research into improved methods for disease diagnosis, treatment or prevention." Preparedness strategies proposed in the literature include the stockpiling of vaccines and personal protective equipment (Adam et al. 2017), restructuring public health organizations and training medical personnel to react to a biological attack (de Almeida 2015), and creating novel platforms for rapid disease diagnostics and vaccine production (Franconi et al. 2018).

One response mentioned mostly in articles concerned with the threat of gene drives and their potential ecological impact was the creation and use of **containment and reversal strategies**, which we identified in 5% of articles. These strategies have been referred to as "risk-reducing innovation" and "built-in safety," and include creating strains of a modified organism that cannot survive outside of the laboratory or can only live on specific substrates to eliminate the threat of accidental release (van de Poel and Robaey 2017), modifying existing genes in a way that allows for the ancestral sequence to be easily restored (i.e. genetic restoration) (Looi et al. 2018), adding susceptibilities to specific treatments or chemicals (i.e., kill switches) that would allow the engineered population to be easily controlled (Wintle et al. 2017), and only building and testing gene drives in geographic areas where the target species is not naturally present (Esvelt et al. 2014). These strategies work to reduce the threat of accidental releases, ecological impacts, and uncertain consequences right at the beginning of the study by building in a way to restore the engineered organism back to its natural state or eliminate it completely.

The final and least frequently mentioned response was **funding**, which appeared in 5% of articles. These articles called for the funding of specific threads of research or institutions that would help to enhance biosecurity. Evans (2014) stated that large "funding bodies have a key role to play reshaping our understanding of what it means to engage in biosecurity governance," and believes that studies looking directly at the social aspects of emerging biotechnology should be funded in their own right and not just as add-ons to other research as has been done previously. He believes that these sorts of studies will allow governance to progress alongside the biotechnology field instead of playing catch-up, but have lacked funding to date. Other calls for funding to increase biosecurity include ensuring that laboratories are financially able to implement proper biosafety precautions (Trevan 2015), offsetting costs for DNA synthesis companies to screen for orders related to pathogens (DiEuliis et al. 2017), and funding biotechnology companies to increase innovation within the nation and decrease the likelihood of these companies moving oversees (Gronvall 2015).

2.4 Conclusion

Biosecurity threats and responses have garnered significant attention and these issues warrant continued investigation and prioritization in order to maximize the benefits and reduce the likelihood of misuse that could cause significant harm to human and environmental health. This review pulls disparate literature together to provide description of the field in sum to date. We envision scholars and decision-makers to use this work to forward new research agendas to better allocate resources toward underdeveloped, yet valuable areas with prescient needs.

By conducting a systematic literature review, we were able to determine which biosecurity threats and responses are most prevalent across this broad field. Dual use research was far and away the most frequently mentioned threat, appearing 29 more times than the second most frequent threat biological weapons. Both of these threats were also prominently evident in the US and EU frameworks developed to address biosecurity concerns evolving out of the use of advanced biotechnology. The US framework also identified information access and lower barriers as biosecurity threats, while the EU framework mentioned the threat of theft by staff ("insider threat") (Trump et al. 2020c). Overall, the US and EU frameworks were concerned with preventing and responding to attacks with biological weapons. While this was a key threat identified in the literature, many of the other threats discussed were more concerned with the potential for negative consequences of authorized releases of engineered organisms into the environment. This accounts for the third most frequently mentioned threat in the literature, ecological impact, which was absent from the governmental frameworks.

Legal oversight was the top response identified in the literature and was also presented as a biosecurity response in both the US and EU frameworks. These frameworks also included other government-driven responses identified in the literature, including surveillance, augmentation of access, improved response capacity, and risk assessment. The EU framework additionally suggested international governance, collaboration, and training/awareness as responses, but these were referring to collaboration and training of governmental agencies (Trump 2017). The top responses identified in the literature that applied more to industry, academia, and the public (open discussions, self-governance and ethics, and education/training/awareness) were noticeably missing from the two governmental frameworks included in this chapter.

This empirical foundation of the prominent areas of concern for biotechnology-related research and discourse may be used to help formulate needs-based considerations for future research. Concise understanding and acknowledgement of the spectrum of concerns related to the proliferation of biotechnological tools can inform regulators and decision-makers who must hold command over contemporary concerns and this work should be used to enable better informed decisions about priority tasks to corral biosecurity threat and foster adaptive responses. As this area continues to gain prominence within communities concerned with biotechnological risk, we anticipate the topics covered here to grow in coverage at an

increasing rate and we anticipate the entrance of yet determined considerations for novel threats and responses. Thus, in due time, we feel a replication of this method and results is warranted to isolate threat and response developments post-2020.

References

Adam DC, Magee D, Bui CM, Scotch M, MacIntyre CR (2017) Does influenza pandemic preparedness and mitigation require gain-of-function research? Influenza Other Respir Viruses 11(4):306–310

Ahteensuu M (2017) Synthetic biology, genome editing, and the risk of bioterrorism. Sci Eng Ethics 23:1531–1561

Baskin CR (2019) Who should be driving US science policy? Perspect Biol Med 62(1):20–30

Bauer MW, Gaskell G (eds) (2002) Biotechnology: the making of a global controversy. Cambridge University Press, Cambridge

Berger KM, Schneck PA (2019) National and transnational security implications of asymmetric access to and use of biological data. Front Bioeng Biotechnol 7:21

Caballero-Hernandez D, Rodriguez-Padilla C, Lozano-Muniz S (2017) Bioethics for biotechnologists: from Dolly to CRISPR. Open Agric 2(1):160–165

Corbin JM, Strauss A (1990) Grounded theory research: procedures, canons, and evaluative criteria. Qual Sociol 13(1):3–21

Cross R (2018) Synthetic biology poses new biosecurity risks. Chem Eng News 16

De Almeida ME (2015) The permanent relation between biology, power and war: the dual use of the biotechnological development. Ciencia & Saude Coletiva 20(7):2255–2266

De Beer J, Jain V (2018) Inclusive innovation in biohacker spaces: the role of systems and networks. Technol Innov Manag Rev 8(2):27–37

DiEuliis D, Giordano J (2017) Why gene editors like CRISPR/Cas may be a game-changer for neuroweapons. Health Secur 15(3):296–302

DiEuliis D, Giordano J (2018) Gene editing using CRISPR/Cas9: implications for dual-use and biosecurity. Protein Cell 9(3):239–240

DiEuliis D, Carter SR, Gronvall GK (2017) Options for synthetic DNA order screening, revisited. MSphere 2:e00319–e00317

Diggans J, Leproust E (2019) Next steps for access to safe, secure DNA synthesis. Front Bioeng Biotechnol 7:86

Duprex WP, Fouchier RAM, Imperiale MJ, Lipsitch M, Relman DA (2014) Gain-of-function experiments: time for a real debate. Nat Rev Microbiol 13:58–64

Edwards B (2014) Taking stock of security concerns related to synthetic biology in an age of responsible innovation. Front Public Health 2:79

Engel-Glatter S, Ienca M (2018) Life scientists' views and perspectives on the regulations of dual-use research of concern. Sci Public Policy 45(1):92–102

Esvelt KM, Gemmell NJ (2017) Conservation demands safe gene drive. PLoS Biol 15(11):e20003850

Esvelt KM, Millett PD (2017) Genome editing as a national security threat. Rev Sci Tech 36(2):459–465

Esvelt KM, Smidler AL, Catteruccia F, Church GM (2014) Concerning RNA-guided gene drives for the alteration of wild populations. Elife 3:e03401

European Commission (2017) Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks. Brussels, Belgium

Evans SG (2014) What's the matter with biosecurity? J Responsib Innov 2(1):88–91

Evans NG, Lipsitch M, Levinson M (2015) The ethics of biosafety considerations in gain-of-function research resulting in the creation of potential pandemic pathogens. J Med Ethics 41(11):901–908

Fear R, ter Meulen V (2016) European academies advise on gain-of-function studies in influenza virus research. J Virol 90(5):2162–2164

Finkel AM, Trump BD, Bowman D, Maynard A (2019) A "solution-focused" comparative risk assessment of conventional and synthetic biology approaches to control mosquitoes carrying the dengue fever virus. Environ Syst Decis 38:177–197

Fonfria E, Elliott M, Beard M, Chaddock JA, Krupp J (2018) Engineering botulinum toxins to improve and expand targeting and SNARE cleavage activity. Toxins 10(7):278

Franconi R, Illiano E, Paolini R, Venuti A, Demurtas OC (2018) Rapid and low-cost tools derived from plants to face emerging/re-emerging infectious diseases and bioterrorism agents. In: Radosavljevic V, Banjari I, Belojevic G (eds) Defense against bioterrorism. Springer, New York

Gomez-Tatay L, Hernandez-Andreu JM (2019) Biosafety and biosecurity in synthetic biology: a review. Crit Rev Environ Sci Technol 49(17):1587–1621

Gomez-Tatay L, Hernandez-Andreu JM, Azner J (2016) A personalist ontological approach to synthetic biology. Bioethics 30(6):397–406

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 (2015) US competitiveness in synthetic biology. Health Secur 13(6):378–389

Hood L, Rowen L (2013) The human genome project: big science transforms biology and medicine. Genome Med 5:79

Imperiale MJ, Casadevall A (2018) A new approach to evaluating the risk–benefit equation for dual-use and gain-of-function research of concern. Front Bioeng Biotechnol 6:21

Imperiale MJ, Howard D, Casadevall A (2018) The silver lining in gain-of-function experiments with pathogens of pandemic potential. Methods Mol Biol 1836:575–587

Jacobsen KX, Mattison K, Heisz M, Fry S (2014) Biosecurity in emerging life sciences technologies, a Canadian public health perspective. Front Public Health 2:198

Jamil SAB (2015) Ethics in synthetic biology: exacerbated misconceptions of the nature of man and cosmology. Asian Bioethic Rev 7(3):331–337

Jefferson C, Lentzos F, Marris C (2014) Synthetic biology and biosecurity: challenging the "myths". Front Public Health 2:115. Front Public Health 2:198

Kozminski KG (2015) Biosecurity in the age of Big Data: a conversation with the FBI. Mol Biol Cell 26(22):3894–3897

Lev O, Samimian-Darash L (2014) Biosecurity policy in the US: a critical assessment. Front Public Health 2:110

Linster M, Boheeman S, de Graaf M, Schrauwen EJA, Lexmond P, Manz B, Bestebroer TM, Baumann J, van Riel D, Rimmelzwaan GF, Osterhaus ADME, Matrosovich M, Fouchier RAM, Herfst S (2014) Identification, characterization, and natural selection of mutations driving airborne transmission of A/H5N1 virus. Cell 157(2):329–339

Looi FY, Baker M, Townson T, Richard M, Novak B, Doran TJ, Short KR (2018) Creating disease resistant chickens: a viable solution to avian influenza? Viruses 10(10):561

MacIntyre CR (2015) Biopreparedness in the age of genetically engineered pathogens and open access science: an urgent need for a paradigm shift. Mil Med 180(9):943–949

MacIntyre CR, Engells TE, Scotch M, Heslop DJ, Gumel AB, Poste G, Chen X, Herche W, Steinhofel K, Lim S, Broom A (2018) Converging and emerging threats to health security. Environ Syst Decis 38:198–207

Mandel GN, Marchant GE (2014) The living regulatory challenges of synthetic biology. Iowa Law Rev 100(1):155–200

Marris C, Jefferson C, Lentzos F (2014) Negotiating the dynamics of uncomfortable knowledge: the case of dual use and synthetic biology. BioSocieties 9:393–420

National Academies of Sciences, Engineering, and Medicine (2018) Biodefense in the age of synthetic biology. The National Academies Press, Washington, DC

Nelson M, Roffey P, McNevin D, Lennard C, Gahan ME (2014) An overview of biosecurity in Australia. Aust J Forensic Sci 46(4):383–396
Noyce RS, Lederman S, Evans DH (2018) Construction of an infectious horsepox virus vaccine from chemically synthesized DNA fragments. PLoS One 13(1):e0188453
Nuclear Threat Initiative (NTI). The Biological Threat (2015). https://www.nti.org/learn/biological/
Oeschger FM, Jenal U (2018) Addressing the misuse potential of life science research – perspectives from a bottom-up initiative in Switzerland. Front Bioeng Biotechnol 6:38
Pastorino B, de Lamballerie X, Cherrel R (2017) Biosafety and biosecurity in European containment level 3 laboratories: focus on French recent progress and essential requirements. Front Public Health 31(5):121
Patton MQ (2014) Qualitative research & evaluation methods: integrating theory and practice. Sage, Thousand Oaks
Polaris Marketing Team (2020) Biotechnology market size, share, trends & analysis report 2020–2026. https://www.polarismarketresearch.com/industry-analysis/biotechnology-market. Accessed 20 Sept 2020
Pope SM (2017) Impact of gene editing tools, like CRISPR/Cas9, on the public health response to disease outbreaks. Disaster Med Public Health Prep 11(2):155–159
Raposo VL (2019) The first Chinese edited babies: a leap of faith in science. JBRA Assist Reprod 23(3):197–199
Redford KH, Adams W, Carslon R, Mace GM, Ceccarelli B (2014) Synthetic biology and the conservation of biodiversity. Oryx 48(3):330–336
Rychnovska D (2016) Governing dual-use knowledge: from the politics of responsible science to the ethicalization of security. Secur Dialogue 47(4):310–328
Sahl JW, Pearson T, Okinaka R et al (2016) A Bacillus anthracis genome sequence from the Sverdlovsk 1979 autopsy specimens. MBio 7(5):e01501-16. Published 27 September 2016. https://doi.org/10.1128/mBio.01501-16
Seager TP, Trump BD, Poinsatte-Jones K, Linkov I (2017) Why life cycle assessment does not work for synthetic biology. Environ Sci Technol 51(11):5861–5862
Stewart IJ (2018) Preventing weapons of mass destruction proliferation: the future of UNSCR 1540. In: Salisbury D, Stewart IJ, Viski A (eds) Preventing the proliferation of WMDs: measuring the success of UN Security Council resolution 1540. Palgrave Pivot, London, pp 105–126
Suk JE, Bartels C, Broberg E, Struelens MJ, Ozin AJ (2014) Dual-use research debates and public health: better integration would do no harm. Front Public Health 2:114
Trevan T (2015) Biological research: rethink biosafety. Nature 527(7577):155–158
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, Cummings CL, Kuzma J, Linkov I (2020a) Synthetic biology 2020: frontiers in risk analysis and governance. Springer, Cham
Trump BD, Galaitsi SE, Appleton E, Bleijs DA, Florin MV, Gollihar JD et al (2020b) Building biosecurity for synthetic biology. Mol Syst Biol 16(7):e9723
Trump BD, Keisler JM, Volk KM, Linkov I (2020c) Biosecurity demands resilience. Environ Sci Technol
UNODA (2017) Biological weapons. https://www.un.org/disarmament/wmd/bio/. Accessed 21 Sept 2020
USDA APHIS (United States Department of Agriculture Animal and Plant Health Inspection Service (2020) Animal disease information. https://www.aphis.usda.gov/aphis/ourfocus/animalhealth/animal-disease-information. Accessed 14 Sept 2020
Van de Poel I, Robaey Z (2017) Safe-by-design: from safety to responsibility. NanoEthics 11:297–306
Verma AS, Agrahari S, Rastogi S, Singh A (2011) Biotechnology in the realm of history. J Pharm Bioallied Sci 3(3):321–323

Vogel KM, Ouagrham-Gormley SB (2018) Anticipating emerging biotechnology threats: a case study of CRISPR. Politics Life Sci 37(2):203–219
Vogel KM, Ozin AJ, Suk JE (2015) Biosecurity and dual-use research: gaining function – but at what cost? Front Public Health 3:13
Walsh PF (2016) Managing emerging health security threats since 9/11: the role of intelligence. Int J Intell Counterintell 29(2):341–367
Webber BL, Raghuc S, Edwards OR (2015) Opinion: is CRISPR-based gene drive a biocontrol silver bullet or global conservation threat? PNAS 112(34):10565–10567
Weidmann AG (2018) Frontiers in CRISPR. ACS Chem Biol 13(2):296–304
Wells E, Trump BD, Finkel AM, Linkov I (2020) A solution-focused comparative risk assessment of conventional and emerging synthetic biology technologies for fuel ethanol. In: Synthetic biology 2020: frontiers in risk analysis and governance. Springer, Cham, pp 223–255
Wintle BC, Boehm CR, Rhodes C (2017) A transatlantic perspective on 20 emerging issues in biological engineering. eLife 14(6):e30247

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.