J Appl Biotechnol Rep. 2026 June;13(2):2024-2034

Journal of
Applied Biotechnology Reports

doi 10.30491/jabr.2025.533238.1889

Thematic Review

Dual Use of Emerging Biotechnologies: Governance and Biosecurity Challenges in the New Era

Mohammd Ebrahim Minaei [1*]

[1] Faculty of Basic Science, Imam Hossein Comprehension University, Tehran, Iran

Corresponding Author: Mohammd Ebrahim Minaei, PhD, Assistant Professor, Faculty of Basic Science, Imam Hossein Comprehension University, Tehran, Iran. Tel: +989352219503, E-mail: mminaii@ihu.ac.ir

Received July 8, 2025; **Accepted** October 22, 2025; **Online Published** June 30, 2026

Abstract

Emerging biotechnologies hold great promise but also pose risks from accidental or deliberate misuse. Assessing these threats requires a systematic approach to examine potential dangers and plan for future developments. Effective biosecurity policies demand an understanding of current biotechnological capabilities and anticipation of their evolution. This qualitative thematic review analyzes biosecurity threats from emerging biotechnologies reported in the scientific literature between 2014-2024. We conducted comprehensive literature searches in PubMed, Scopus, and Google Scholar using terms related to core biotechnologies (e.g., "synthetic biology," "gene editing") and threat concepts (e.g., "biosecurity," "dual-use"). Relevant publications were analyzed to identify and synthesize recurring themes and governance challenges. The analysis identified dual-use potential as the most prominent biosecurity concern associated with emerging biotechnologies. The review synthesizes the literature to critically evaluate key threats, including biological weapons, environmental impacts, and governance challenges. It further discusses how national and global biosecurity policies can be adapted to maximize the benefits of these technologies while minimizing risks. Establishing governance policies to bridge the gap between the security of previous-generation biotechnology and the scientific and technological capabilities of the next decade's emerging biotechnologies, as well as to maximize the benefits of deploying and minimize the potential for dual use of emerging biotechnologies, is essential to address the challenges and concerns associated with emerging biotechnologies.

Keywords: Biosecurity, Emerging Biotechnologies, Dual Use, Governance, Biological Agents

Citation: Minaei ME. Dual Use of Emerging Biotechnologies: Governance and Biosecurity Challenges in the New Era. J Appl Biotechnol Rep. 2026;13(2):2024-2034. doi:10.30491/jabr.2025.533238.1889

Introduction

Research in emerging biotechnologies has grown remarkably in the past decade. The pace of advancement in emerging biological sciences and technologies is now faster than ever, but so too are their potential harmful and destructive capabilities. Emerging biotechnologies have numerous applications in health and medicine (new vaccines, drug delivery, healthcare), energy (biofuels), environmental remediation, agriculture, food production, and general industry (detergents, adhesives, etc.).[1,2]

Potential future applications of emerging biotechnologies in health and medicine include advanced diagnostics based on a comprehensive understanding of life processes, development of cheaper, faster-acting and improved therapeutics (including point-of-care treatments) such as personalized medicines, smart wound-healing materials, cyber-genetics, enhanced safety monitoring, production of antibiotics, vaccines and other biological products (including metabolic regulators), human enhancement, development of augmented organs ("superhuman"), creation of artificial organelles to compensate for natural deficiencies (e.g., insulin delivery for diabetics), engineered microbiomes for self-regulation, improved performance, health or stronger immune systems, or more efficient nutrient processing from food, development of climate-resilient and pest-resistant crops to address challenges from climate change and food shortages due to population growth, remote health and environmental monitoring, and production of enhanced food products with extended shelf life.[3,4]

On the other hand, emerging biotechnologies can also be used for destructive purposes by terrorist organizations or hostile nations to create dangerous pathogens, invasive organisms or other harmful biological agents.[5] This dual-use potential makes emerging biotechnologies a research area with both beneficial and harmful applications.[6] In fact, there have been 35 confirmed cases of biological weapons use between 1970-2014, with state actors primarily responsible for employing emerging biotechnologies for weapons development.[7] However, emerging biotechnologies are expected to become an even greater concern in the future as advances enable the design, development and deployment of

novel pathogenic biological weapons with characteristics distinct from natural pathogens.[8]

Biological weapons created through emerging bio-technologies present unique new threats. These potential threats include enhanced pathogen transmission across and within species, resistance to existing treatments, engineering of normally benign microbes to produce toxic biological compounds, revival of extinct pathogens, and creation of novel microorganisms. Key sciences and technologies of concern in the near future are predicted to include synthetic biology, oligonucleotide synthesis, DNA assembly (combining smaller oligonucleotide fragments into desired larger sequences), genetic modification (editing, deletion), targeted insertion of desired sequences into genomic locations, biomarkers, personalized medicine (treatments based on individual genetic and biological characteristics), stem cells, and artificial intelligence in life sciences.[9,10]

Developing effective biosecurity policies and procedures to protect humans, agriculture, technology, industry, and the environment against misuse (whether accidental or intentional) requires an understanding of the current state of emerging biotechnologies. This includes knowledge of existing sciences and technologies for manipulating or creating new biological agents (such as viruses, microbes, multicellular organisms or cell-free systems) and planning for future developments. Biosecurity requires developing screening mechanisms for synthetic pathogens and biological attacks, as well as assessment methods (Figure 1).

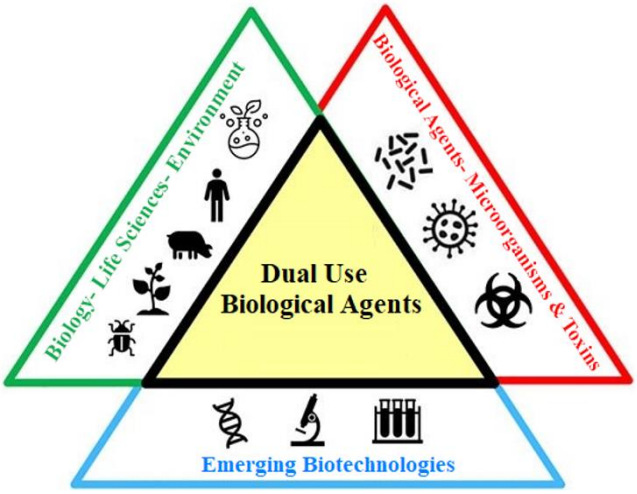

Figure 1. Dual-Use Potential of Biological Agents in Emerging Biotechnologies.[10]

Methods

We conducted comprehensive literature searches using terms related to advanced scientific fields, including:

- Core technologies: "synthetic biology," "gene drives," "gene editing" (particularly CRISPR-based systems), and "cell-free systems"
- Threat-related terms: "biosecurity," "biological weapons," "biological defense," "bioterrorism," and "dual-use biological agents"

The searches were performed across multiple databases (PubMed, Scopus, ResearchGate) and Google Scholar, limited to English-language publications. We excluded articles that:

- Focused solely on technical aspects without security implications
- Addressed biosecurity concerns unrelated to advanced biotechnologies

From an initial pool of search results, relevant full-text articles published between 2014-2024 were selected for in-depth analysis. Moving beyond a quantitative count, this review adopts a thematic synthesis approach. The analysis involved a close reading of the literature to identify, analyze, and report patterns (themes) within the data. Instead of categorizing articles into discrete quantitative bins, the focus was on interpreting and synthesizing the arguments, concerns, and proposed solutions presented across the body of literature. This methodology allows for a nuanced exploration of the relationships between technological capabilities, their potential misapplications, and the corresponding governance dilemmas, providing a critical perspective on the biosecurity landscape that a quantitative tally cannot offer. Following established frameworks for assessing emerging risks, we implemented a two-phase analysis:

1. Literature Identification and Screening: A comprehensive search of scientific databases (PubMed, Scopus, Google Scholar) was conducted for English-language articles published between 2014-2024, using a combination of keywords related to biotechnology fields and biosecurity concepts.
2. Thematic Synthesis: The full texts of relevant articles were analyzed to identify, categorize, and synthesize recurring themes, concerns, and proposed governance solutions. Instead

of quantitative counts, the analysis focused on understanding the relationships between technological capabilities, potential misuses, and the corresponding governance challenges discussed in the literature. This qualitative synthesis provides a nuanced understanding of the biosecurity landscape, moving beyond a summary of individual articles to critically evaluate connections between identified threats and solutions.

Results

Analysis and Synthesis: Thematic Biosecurity Threats and Governance Challenges

The analysis of the literature reveals that concerns surrounding emerging biotechnologies are not isolated but interconnected, centering on the fundamental tension between their beneficial potential and inherent risks. The following synthesis organizes these concerns into key thematic areas, critically evaluating the literature to connect identified threats with their underlying governance challenges.

1. The Pervasive Challenge of Dual-Use Potential:

The most extensively discussed theme is the dual-use nature of nearly all advanced biotechnologies. In reports, dual-use research is defined as: "biological sciences research that, based on current understanding, can be reasonably anticipated to provide knowledge, information, products, or technologies 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, materiel, or national security." Other researchers note that "any powerful tool that creates significant capability with at least some risk (if not threat) can be used to exert influence or achieve various objectives".[11,12] Most emerging biotechnology research is beneficial and legitimate, conducted to benefit society. However, the same knowledge and techniques from beneficial research can be misused destructively. For example, CRISPR-Cas9 gene editing is used therapeutically for cancer treatment, improving cancer therapy while reducing reliance on toxic chemotherapy, but could also be used to enhance pathogen virulence.[13,14] This duality presents a core governance challenge: fostering innovation while implementing oversight mechanisms that are effective without being stifling. The debate around Gain-of-Function (GOF) research exemplifies this tension, where the value of scientific knowledge must be weighed against the risk of creating potentially dangerous information. Some dual-use research in emerging biotechnologies involves gain-of-function (GOF) studies. Duprex et al.[15,16] define GOF as "a general label for a wide range of experiments that result in a genetically modified biological agent with novel or enhanced functional properties." Concerns about GOF research include studies on avian influenza viruses and poxviruses. Publication of such studies is itself considered a biosecurity threat, as the information could enable biological weapons development - referred to as "information access".[17,18]

2. From State Actors to Individuals:

The Evolving Nature of the Threat Actor: Closely linked to dual-use is the theme of evolving threats from biological weapons. The literature describes a shift from traditional state-sponsored programs to potential misuse by non-state actors or even individuals, facilitated by the increasing accessibility and decreasing cost of core technologies. Previously weaponized organisms like those used in the 2001 anthrax attacks could re-emerge as threats through emerging biotechnologies. Kress[19] outlines three ways emerging technologies could be used to create biological weapons: 1) Recreating pathogenic viruses (e.g., Ebola, SARS, smallpox); 2) Engineering bacteria to be more dangerous (e.g., adding antibiotic resistance genes); 3) Modifying microbes to produce and disseminate toxic biochemical. Researchers have demonstrated capabilities in all three areas: horsepox virus synthesized from mail-order DNA;[20] avian influenza engineered for airborne transmission between mammals;[21] and botulinum toxin produced in yeast cells.[22] These examples also highlight dual-use research, being conducted for beneficial purposes (vaccine development, transmission studies, and enhanced therapies respectively).

While biological weapons and bioterrorism primarily involve the intentional release of engineered pathogens or toxins, accidental release of modified organisms is also identified as a threat in technical literature, typically classified as a biosafety rather than biosecurity concern.

This democratization of capability necessitates a parallel evolution in governance, moving beyond state-centric models to include bottom-up approaches, such as codes of conduct within the DIY-bio community, and enhanced screening of genetic material orders.

3. Environmental and Ecological Uncertainties:

A significant theme involves the potential for irreversible environmental impacts, particularly related to gene drive technologies.[23,25] The literature highlights a critical governance gap: the lack of international frameworks for assessing and managing cross-border ecological risks. While gene drives offer potential benefits like controlling disease vectors, the scientific consensus points to significant uncertainty regarding their long-term ecological consequences, raising questions about sovereignty and liability if modified organisms spread beyond national borders. Although biological weapons could directly target critical environmental components, ecological concerns mainly stem from the increasing use of engineered organisms for pest control and recent advances in gene drive technology. Wiedemann[23] defines gene drives as "experimental techniques designed to introduce foreign genes into wild population chromosomes

with the goal of completely altering organisms within a few generations." Potential beneficial applications include reducing populations of mosquitoes transmitting dengue and malaria.[24]

However, since organisms and viruses can reproduce, mutate and share genes, there is no guarantee that modifications will remain confined to target populations, nor can ecological cascade effects be reliably predicted. This inherent uncertainty makes advanced biotechnology a potential threat to ecosystems, as extensively discussed in the literature. Wiedemann considers gene drives "ethically dubious since we don't yet know whether genetic changes might harm other organisms or entire ecosystems".[23] Wintle et al.[25] similarly warn that "gene drive deployment in wild populations could disrupt ecosystems, trophic networks and food webs, creating niches for new disease vectors or pathogens." Weber et al.[26] conclude that "species elimination via gene drives may trigger unintended cascades potentially more threatening than target species." Overall, concerns about irreversible negative impacts of genetically modified species on entire ecosystems were prominent in the reviewed literature.

Ecological systems exhibit complex, poorly understood interactions (from global to cellular levels), and advanced biotechnology remains a rapidly developing field with few field trials of engineered organisms.[27] When these complex components interact, experts worry that the consequences cannot be reliably predicted or prevented. Esvelt and Gemmell.[28,29] highlight national sovereignty issues, where the cross-border spread of engineered species could violate sovereignty and damage diplomatic relations.

Most concerning emerging biotechnologies in literature include:

- **Binary biological weapons:** A two-component system combining a pathogenic host strain with plasmid-carried virulence genes, mixed just before deployment in munitions functioning as bioreactors.[30]
- **Designer genes:** Following the Human Genome Project's completion, synthetic biology now enables the design of novel pathogens from published sequences.[30]
- **Stealth viruses:** Can remain dormant in specific individuals until activated by environmental triggers.[31]
- **Host-switching diseases:** Animal viruses genetically modified to infect humans.[32]
- **Designer Diseases:** Cellular manipulation to induce uncontrolled proliferation or programmed cell death.[30]
- **Personalized Bioweapons:** Pathogens targeting specific genomic profiles.[30]
- **Neuroengineering:** Nervous system manipulation for mind control or non-lethal weapons.[30]

Types of Biological Threats from a Biosecurity Perspective

Biological threats related to emerging biotechnologies fall into two primary categories: biosafety threats (resulting from accidents or negligence) and biosecurity threats (stemming from intentional misuse of knowledge, information, or materials). The critical importance of laboratory safety when working with these technologies is widely acknowledged. Since the initial genetic engineering experiments of the 1970s that prompted calls for a research moratorium, extensive debates about recombinant DNA (rDNA) work led to an international agreement to continue such research under stringent containment protocols.

The "Global Science Conduct: Guide for Responsible Behavior in the Global Research Enterprise" explicitly addresses laboratory and environmental safety, serving as a vital resource for promoting research integrity standards. Professional biosafety organizations play a crucial role in advancing safe biological research practices through support services, capacity development, certification programs, and professional networking.[33]

For all industries, developing safe, high-quality products represents both a priority and responsibility. The Biotechnology Innovation Organization, representing private and public companies and academic institutions across the U.S. and 30+ countries, launched the pioneering "Excellence Through Stewardship" program in 2007 as the first coordinated industry initiative. Contrary to some assumptions, the DIY biology community has actively incorporated biosafety protocols, establishing responsible codes of conduct tailored to their specific working environments. Biosecurity, like biosafety, encompasses multiple definitions. The World Health Organization defines laboratory biosecurity as protective measures and accountability protocols for biological materials to prevent unauthorized access, theft, misuse, or intentional release. More broadly, biosecurity involves minimizing risks where life sciences could be misused (accidentally or deliberately) to harm humans, animals, plants, or ecosystems - including threats from bioterrorism, biological crimes, and biological weapons development.[34]

Biosecurity concerns have gained prominence over the past decade, particularly given the global proliferation of dual-use capabilities. Seminal studies demonstrating the need for a comprehensive assessment of emerging bio-technologies' societal, ethical, and legal implications include the accidental enhancement of mousepox virulence, artificial poliovirus synthesis, reconstruction of the 1918 influenza virus, and creation of synthetic life forms.

Two influential U.S. National Research Council reports (2004, 2006) provided key recommendations in this field. The Fink Committee Report ("Biotechnology Research in an Age of Terrorism") identified seven experiment types requiring expert review before execution or publication: Vaccine neutralization, Conferring antimicrobial resistance, Pathogen virulence enhancement or creation, Increased pathogen transmissibility, Altered host range, Diagnostic/ detection evasion, Biological agent/toxin weaponization.

The Lemon-Relman Report ("Globalization, Biosecurity, and the Future of the Life Sciences") proposed a framework for evaluating dual-use potential, categorizing technologies into four groups: a) Those seeking novel biological/ molecular diversity, b) Those producing predetermined biological/molecular entities, c) Those manipulating biological systems comprehensively, and d) Those enhancing production /delivery of bioactive materials.[35]

The report advocates a "threat spectrum" approach focusing on life science advances enabling dual-use applications. Unlike biosafety issues, biosecurity threats may not be immediately obvious to researchers, as illustrated by the international controversy surrounding the mammalian-transmissible H5N1 virus (2011).[35]

Effective biosecurity requires understanding both weaponizable technologies and potential targets.[36] The CDC classifies disease transmission as:

- **Direct:** Person-to-person contact or exposure to infected environmental reservoirs, including droplet transmission (e.g., COVID-19, pneumonic plague)[37]
- **Indirect:**
  Vehicle-borne (contaminated objects/materials)
  Vector-borne (organism-mediated)
  Airborne (aerosolized particles)[38]

The 2001 anthrax attacks (mail-borne) and 1984 Rajneeshee salmonella contamination (food-borne) demonstrate vehicle-borne threats. Modeling suggests milk supply contamination could affect hundreds of thousands.[39] Agricultural systems remain vulnerable to object-mediated transmission.[40,41]

While vector-borne transmission (e.g., mosquito-borne diseases) represents a natural outbreak mechanism, its deliberate use remains challenging due to logistical constraints.[42] Most emerging human pathogens originate from animals,[7] yet biological attack planning has largely overlooked animal vectors.

Airborne transmission has received particular attention for bioweapon potential.[43] U.S. military tests (1950s-60s) demonstrated wide-area dispersion of biological aerosols (Operation LAC). Modern concerns include drone-based dispersal or concealed aerosol devices in crowded spaces.[43,44]

Governance and Effective Policy for Biosecurity

Since emerging biotechnologies have dual-use applications, governments must weigh the risks of misuse against their potential benefits for innovation and development. Biosecurity efforts face uncertainties regarding the actual capabilities of these technologies and the motivations of their users, especially as their applications expand across various fields. Many advanced governments still rely on outdated regulations to govern new technologies, which is an inadequate strategy for ensuring security in the coming decades.[45]

Developing an effective biosecurity strategy for emerging biotechnologies requires understanding the innovations introduced by fields such as synthetic biology, gene drives, and gene editing, as well as the causes of inadequate biosecurity practices and the vulnerabilities stemming from their dual-use nature. New biosecurity concerns arise from their broad scope, increasing accessibility, complexity, dual-use potential, and uncertainties about current and future capabilities. For example, CRISPR-based gene editing represents a major leap forward in genetic engineering, with the potential to revolutionize human health and environmental research. However, it also carries risks of significant and irreversible harm, including the uncontrolled spread of edited genes in the environment, ecosystem disruption by genetically modified organisms (particularly engineered gene drives), and unintended off-target genetic modifications.[46]

Alongside three major international health organizations - the World Health Organization (WHO), the Food and Agriculture Organization (FAO), and the World Organization for Animal Health (OIE), which operate under the United Nations (UN) framework - the U.S. National Institutes of Health (NIH) established early guidelines for genome engineering in 1975, enforced through funding restrictions. However, many biologists can conduct research without significant funding, NIH approval, or even NIH oversight, and the NIH's authority does not extend globally. Today, the financial costs, time requirements, and technical expertise needed for emerging biotechnologies have decreased to the point where some tools are accessible even to elementary school students. Additionally, the foundational knowledge required has diminished as biotechnological processes become simpler. While widespread access to genetic engineering tools can accelerate scientific progress, it shifts the burden of biosecurity onto governments in the absence of global oversight. In 2018, the Secretariat of the Biological Weapons Convention (BWC) expressed concerns about the increasing accessibility of gene editing, gene drives, and gene synthesis technologies to actors with little or no oversight from industry or governments, raising the risk of BWC violations. While predicting and mitigating emerging threats at various scales is valuable, international treaties lack mechanisms to monitor bottom-up efforts in the localization and globalization of emerging biotechnologies below the national level. One possible solution could involve expanding the role of established regulatory bodies such as the WHO, FAO, OIE, and NIH.[47]

Regulatory processes alone cannot fully oversee biotechnological research, so responsible governance requires transparent and coordinated R&D processes, international collaboration on biotechnological challenges, and ethics training for researchers. Complementing regulatory measures, the Responsible Research and Innovation (RRI) approach - adopted by the UK and the European Union - evaluates the societal and environmental impacts of new research to align outcomes with public expectations. Under RRI, multidisciplinary

experts assess scientific developments to mitigate risks, ensure equitable and sustainable access to advancements, and uphold ethical standards. Programs using this approach do not seek to restrict research or publication but aim to minimize downstream harms that could impose cleanup costs and liabilities on developers, companies, or governments. Although RRI is a key criterion for public funding, it remains voluntary rather than a legal requirement.[47]

Currently, biosecurity is treated as a voluntary commitment, requiring individuals, organizations, and companies to allocate their resources to address complex and often conflicting security needs. This precarious cost-benefit balance incentivizes institutions to minimize oversight-related expenses.[48] The strongest argument for investing in biosecurity is that emerging biotechnologies ultimately require public approval. Yet, current public skepticism raises concern about their safety.[49]

A long-term risk-based analysis of biosecurity policies reveals significant gaps in addressing emerging biotechnologies. These shortcomings include: a) Treating security as an undesirable cost to be minimized, b) Reinforcing silos between government, industry, academia, and civil society, and c) Operating within a limited framework that overlooks technological advancements in different countries.

Each of these issues can be addressed through policies that encourage technological development while mitigating security threats, fostering public engagement, and promoting market investment in emerging biotechnologies. Effective policies in this field must be feasible, adaptable, and scalable to address evolving technical and social challenges.

Globalization and the expanding distribution of biotechnological research and products exacerbate challenges posed by differing global governance approaches. Europe and the U.S. no longer dominate advanced biological research, as developed countries adopt varying biosecurity priorities and methods. For example, Russia's 2019–2027 Federal Research Program for Genetic Technology Development aims to *"provide comprehensive solutions for the rapid development of genetic technologies, including gene editing, and establish scientific and technological foundations for medicine, agriculture, and industry while enhancing biological emergency prevention and monitoring systems"* (Russian Ministry of Science and Higher Education, 2019). Similarly, Saudi Arabia funds research on microbial cell factories for fuel and chemical production, while Singapore heavily invests in life sciences and environmental research at institutions such as Nanyang Technological University, the National University of Singapore, and the Agency for Science, Technology, and Research. China's Academy of Sciences is establishing an Institute of Synthetic Biology to develop a roadmap for the country's synthetic biology future while setting safety and security standards for researchers. Beyond existing frameworks like the BWC or the Chemical Weapons Convention (CWC), there are no top-down mechanisms to standardize global governance of emerging biotechnologies (Figure 2).[47]

Developing countries may face different risk structures regarding emerging biotechnologies compared to developed nations. The implications of their involvement in this field can be broadly categorized into two areas:

- Varied safety and security practices across the international supply chain, which underpins the globalized economy.
- The potential for small-scale experiments or national biosecurity policies to escape a country's control and spill across political borders.[50]

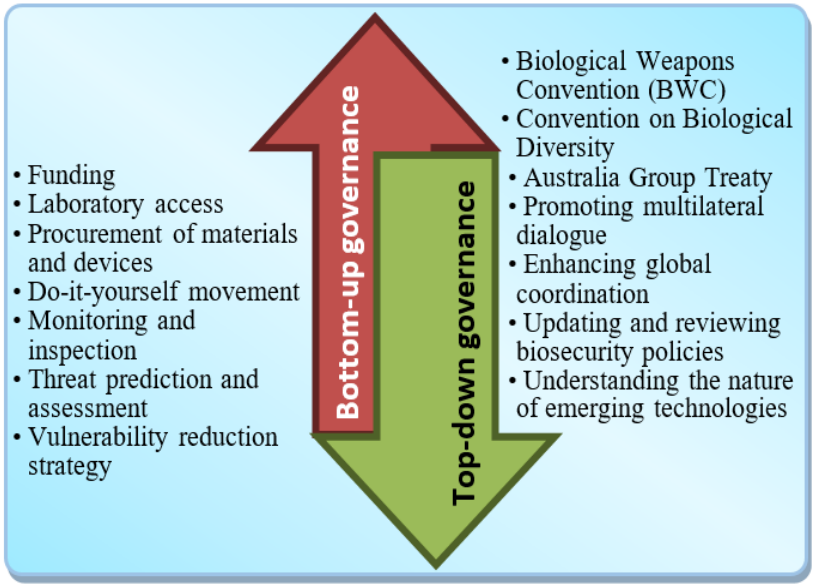

Figure 2. Top-Down and Bottom-Up Governance Policies to Maximize Benefits and Minimize Dual-Use Potential of Emerging Biotechnologies.

While one country may deem the environmental risks of a biotechnological application acceptable, its cross-border spread could disrupt ecosystems or expose vulnerable populations to irreversible consequences. Risk-averse countries (e.g., those concerned about gene drives) cannot fully isolate themselves from harm caused by another nation's decisions. Risk-tolerant countries may reap the benefits of successful technologies, while risk-averse ones may bear the risks without sharing in the rewards. Governments, organizations, and industries may define security threats and acceptable risk levels differently when pursuing technological advancements. For emerging biotechnologies, such policy divergence could lead to fragmented approaches, hindering consensus on specialized concerns or security assessment protocols.[47]

Biosecurity of Dual-Use Emerging Biotechnologies Based on the Experimental Governance Model

Due to the unpredictability of anthropogenic risks associated with dual-use emerging biotechnologies, information asymmetry, and insufficient awareness of misuse risks, top-down and bottom-up governance policies may face disruptions. To address this gap, a corresponding governance mechanism called experimental governance is proposed. Experimental governance is a multi-layered management approach aimed at institutionalizing policies into social practices based on local conditions.[51] In 2008, Sabel and Zeitlin first introduced the theory of experimental governance, inspired by the European Union's recursive learning approach in adapting to international conventions.[52,53] Since then, experimental governance has been applied to global governance, with other researchers enhancing this dynamic framework through goal-setting, reporting requirements, peer review, and consultative processes.[54]

Given high uncertainty and implementation costs, Sabel and Victor[55] institutionalized global experimental governance by setting conditional objectives under appropriate processes, subject to ongoing review, revision, and improvement. Such governance measures must rely on strong institutional support (e.g., deferred penalties to increase the likelihood of success). The experimental governance model consists of four stages:

Stage 1: Achieving Consensus on a Global Governance Framework

The first step involves engaging all stakeholders in discussions, establishing an internationally recognized platform for dialogue, ensuring inclusive participation, and creating a legally binding agreement. The UN Biological Weapons Convention (BWC) can facilitate inter-state communication and provide opportunities for non-state actors to contribute through expert meetings, side events, and best-practice sharing to systematically monitor scientific and technological advancements. For dual-use biotech risk assessment, stakeholders must agree on three principles:

a) Risk Communication: Defined by the U.S. National Research Council as "an interactive process of exchanging information and ideas among individuals, groups, and institutions".[56] It resolves conflicts arising from differing risk perceptions among the public, governments, scientists, and industries.
b) Transparent Oversight: Critical throughout bioscience research. Researchers working with high-risk pathogens (WHO Risk Groups 3/4), high-containment labs (BSL-3+), or vaccine and biopharmaceutical production must submit experimental protocols, methods, and contingency plans for approval before commencing. A "project initiation-review-execution-verification" oversight chain ensures accountability.
c) Systematic Awareness and Training: Essential for fostering a culture of safe and responsible research in dual-use biotechnology.

Stage 2: National Adaptation Based on Local Conditions

Countries must enhance three aspects according to their specific contexts:

a) Balancing Hard and Soft Law:
   - Soft law (guidelines, standards, professional codes) is crucial early in research to promote responsible conduct.
   - Hard law (regulations, statutes) becomes necessary as technologies industrialize.
   - A dynamic regulatory mechanism integrating both is needed for effective risk prevention.[57]
b) Establishing Dynamic Consultative Mechanisms:
   - Governance should emerge from socio-political interactions involving collective stakeholder input.[58,59]
   - Biologists can form "independent networks" combining expertise from multiple institutions to align interests.[60]
c) Hierarchical Risk Management and Assessment:
   - Countries should implement tiered risk management (e.g., China's 2020 *Biosecurity Law* classifies biotech R&D into high, medium, and low-risk categories based on potential harm.[61]
   - The U.S. National Science Advisory Board for Biosecurity (NSABB) focuses on 15 high-risk pathogens and seven dual-use research types.[62,63]
   - Scenario-based risk assessment models.[64]

Stage 3: Transnational Information Sharing and Review

International organizations (e.g., WHO, FAO) must monitor national implementation of dual-use biotech policies, ensuring alignment between bottom-up and top-down governance. A dynamic consultative mechanism for transnational data sharing enables self-regulation and policy coherence (Figure 3).

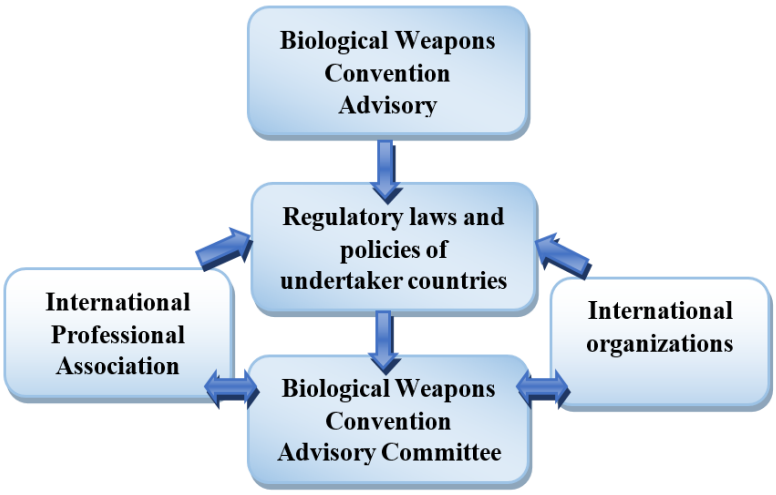

Figure 3. Dynamic Negotiation Mechanism for Transnational Information Sharing.

Stage 4: Global Framework Evaluation and Adjustment

Based on consensus-building, local adaptations, and multilateral reviews, experimental governance iteratively updates global mechanisms. Post-COVID-19, heightened attention to global health security offers policy windows for strengthening international cooperation.[65] Despite geopolitical tensions, many governments prioritize collaborative solutions, creating opportunities for emerging biotechnologies to contribute to sustainable development (Figure 4).

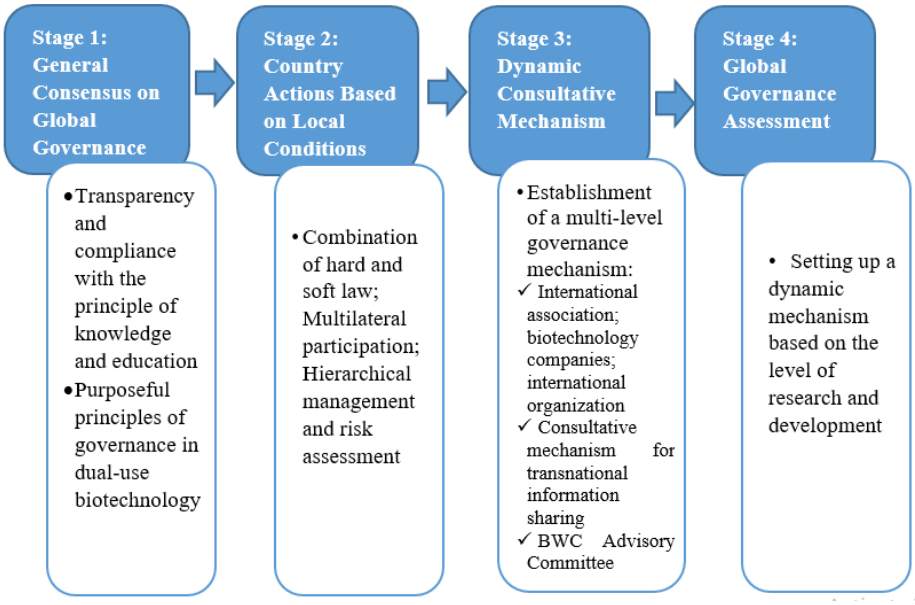

Figure 4. Global Experimental Governance Model for Dual-Use Biotechnologies.

Conclusion

This thematic review synthesizes the current discourse on biosecurity and emerging biotechnologies, highlighting that the primary challenge is governance fragmentation in the face of rapidly evolving, dual-use capabilities. The analysis demonstrates that effective policy must move beyond reactive measures and embrace adaptive, multi-stakeholder approaches. Current global readiness to address emerging biosecurity challenges - including advanced strategies in biotech and AI - remains inadequate. In Iran, the rapid growth of biotechnology in vaccine development and agriculture necessitates tailored biosecurity policies for emerging technologies. A multi-layered regulatory approach (e.g., experimental governance) should be integrated into national planning.

Emerging biotechnologies pose critical challenges: outpacing policy reforms, incomplete risk assessments due to private-sector dominance, and blurred lines between peaceful use and intentional misuse. Literature highlights dual-use biological agents as the most frequent threat,

underscoring a global problem requiring high-level policy attention. While targeted countermeasures can mitigate risks, preventive actions will be more effective long-term. Biosecurity policies must evolve to address unprecedented challenges and the globalized nature of these threats.

The synthesis of literature from the past decade clearly indicates that effective governance must be as adaptive and dynamic as the technologies it aims to oversee. Simply recognizing the dual-use dilemma is insufficient; policies must be operationalized through concrete mechanisms. Therefore, this analysis leads to the following specific, actionable recommendations:

1. Implement Mandatory, Project-Specific Dual-Use Risk Assessments: Funding agencies and scientific journals should make it a requirement for researchers working with specified high-concern techniques to complete a standardized dual-use risk assessment at the grant application and manuscript submission stages. This moves beyond voluntary guidelines to create a systematic screening layer.

Misuse incentives are high, and harmful consequences for health and the environment may soon materialize. Successful biosecurity must be adaptive, accommodating new uncertainties. Urgent action is needed to operationalize these concepts before a crisis triggers restrictive policies that could stifle research or drive it underground.

In North America and Europe, biosecurity is prioritized through independent and governmental initiatives, such as the DIY biology movement's ethical codes. However, incentivizing private-sector investment remains unresolved. Potential solutions include training journal editors to screen for risky data and requiring grant applicants to assess security risks.

2. Develop an International Protocol for the Environmental Release of Engineered Organisms: Bodies like the Convention on Biological Diversity (CBD), in coordination with the BWC, must pioneer a formal protocol for the transparent risk assessment, notification, and monitoring of any proposed environmental release of gene drive organisms or other persistent biological modifications, establishing liability and response frameworks for cross-border incidents.

A hybrid top-down (international treaties like the BWC) and bottom-up (grassroots monitoring) approach is essential, though current frameworks face funding and enforcement gaps. While no policy can eliminate all threats, a layered strategy involving governments, private entities, and researchers can reduce regulatory gaps. Proposed measures include:

- A comprehensive strategy for data collection/analysis on emerging biotech.
- Shared classified information frameworks.
- Enhanced communication to expose BWC violations.
- Public-private partnerships to identify risks in supply chains and research.

3. Integrate Biosecurity "By Design" into Education and Funding: University curricula for life sciences and engineering degrees should incorporate mandatory modules on responsible innovation and biosecurity. Simultaneously, funding programs should incentivize the development of technical safeguards (e.g., genetic "use controls") that embed safety and security directly into biological systems.

In conclusion, safeguarding the promise of emerging biotechnologies demands a shift from discussing governance to experimentally implementing it. The proposed experimental governance model, with its emphasis on iterative learning and multi-stakeholder engagement, provides a flexible framework for this effort. The time for proactive governance is now, before a crisis forces a reaction that may undermine both security and scientific progress.

Aligning national and global biosecurity principles can make emerging technologies safer, more responsible, and more trusted. Multilateral discourse, improved coordination, and adaptive governance mechanisms are key to bridging the gap between outdated policies and next-generation biotech capabilities.

Conflict of Interest Disclosures

The authors declare that they have no conflicts of interest.

References

1. Lowe R, Minssn T, Skentelbery C. Emerging Biotechnologies in Europe: Foresight for Policy. Publications Office of the European Union. 2024.
2. Cabling M, Marciniak-Nuqui Z, Marjanovic S. (RAND Europe): Microbiome-Based Health and Wellness Innovation: Reflecting on Regulatory Challenges and Needs. 2022.
3. Evans NG, Selgelid MJ. Biosecurity and open-source biology: the promise and peril of distributed synthetic biological technologies. Sci Eng Ethics. 2015;21(4):1065-83. doi:10.1007/s11948-014-9591-3
4. Bier E. Gene drives gaining speed. Nat Rev Genet. 2022;23(1):5-22. doi:10.1038/s41576-021-00386-0
5. Kwik Gronvall G. Biosecurity: the opportunities and threats of industrialization and personalization. Bull at Sci. 2015;71(6):39-44. doi:10.1177/0096340215611086
6. Getz LJ, Dellaire G. Angels and devils: dilemmas in dual-use biotechnology. Trends Biotechnol. 2018;36(12): 1202-5. doi:10.1016/j.tibtech.2018.07.016
7. Franconi R, Illiano E, Paolini F, Massa S, Venuti A, Demurtas OC. Rapid and low-cost tools derived from plants to face emerging/re-emerging infectious diseases and bioterrorism agents. In Defence Against Bioterrorism: Methods for Prevention and Control. Dordrecht: Springer Netherlands. 2018. pp. 123-139. doi:10.1007/978-94-024-1263-5_10
8. Gronvall G. The security implications of synthetic biology. In Survival 60.4. Routledge. 2023. pp. 165-180.
9. Linkov I, Trump BD, Anklam E, Berube D, Boisseasu P, Cummings C, et al. Comparative, collaborative, and integrative risk governance for emerging technologies. Environ Syst Decis. 2018;38(2):170-6. doi:10.1007/s10669-018-9686-5

10. Holzinger A, Keiblinger K, Holub P, Zatloukal K, Müller H. AI for life: Trends in artificial intelligence for biotechnology. New Biotechnol. 2023;74:16-24.
11. Lev O, Samimian-Darash L. Biosecurity policy in the US: a critical assessment. Front Public Health. 2014;2:110. doi:10.3389/fpubh.2014.00110
12. DiEuliis D, Giordano J. Gene editing using CRISPR/Cas9: implications for dual-use and biosecurity. Protein Cell. 2018;9(3):239-40. doi:10.1007/s13238-017-0493-4
13. Vogel KM, Ouagrham-Gormley SB. Anticipating emerging biotechnology threats: A case study of CRISPR. Politics Life Sci. 2018;37(2):203-19. doi:10.1017/pls.2018.21
14. Spasskaya DS, Davletshin AI, Bachurin SS, Tutyaeva VV, Garbuz DG, Karpov DS. Improving the on-target activity of high-fidelity Cas9 editors by combining rational design and random mutagenesis. Appl Microbiol Biotechnol. 2023;107(7):2385-401. doi:10.1007/s00253-023-12469-5
15. Duprex WP, Fouchier RA, Imperiale MJ, Lipsitch M, Relman DA. Gain-of-function experiments: time for a real debate. Nat Rev Microbiol. 2015;13(1):58-64. doi:10.1038/nrmicro3405
16. Greek I. The truth about gain-of-function research. Nature. 2021;598. doi:10.1038/d41586-021-02903-x
17. DiEuliis D, Carter SR, Gronvall GK. Options for synthetic DNA order screening, revisited. MSphere. 2017;2(4):10-128. doi:10.1128/msphere.00319-17
18. Jamil SA. Ethics in synthetic biology: exacerbated misconceptions of the nature of man and cosmology. Asian Bioethic Rev. 2015;7(3):331-7.
19. Cross R. Synthetic biology poses new biosecurity risks. Chem Eng News. 2018;16.
20. Noyce RS, Lederman S, Evans DH. Construction of an infectious horsepox virus vaccine from chemically synthesized DNA fragments. PloS One. 2018;13(1): e0188453. doi:10.1371/journal.pone.0188453
21. Linster M, van Boheemen S, de Graaf M, Schrauwen EJ, Lexmond P, Mänz B, et al. Identification, characterization, and natural selection of mutations driving airborne transmission of A/H5N1 virus. Cell. 2014;157(2):329-39. doi:10.1016/j.cell.2014.02.040
22. Fonfria E, Elliott M, Beard M, Chaddock JA, Krupp J. Engineering botulinum toxins to improve and expand targeting and SNARE cleavage activity. Toxins. 2018;10(7):278. doi:10.3390/toxins10070278
23. Weidmann AG. Frontiers in CRISPR. ACS Chem Biol. 2018;13:296–304. doi:10.1021/acschembio.8b00135
24. Finkel AM, Trump BD, Bowman D, Maynard A. A "solution-focused" comparative risk assessment of conventional and synthetic biology approaches to control mosquitoes carrying the dengue fever virus. Environ Syst Decis. 2018;38(2):177-97. doi:10.1007/s10669-018-9688-3
25. Wintle BC, Boehm CR, Rhodes C, Molloy JC, Millett P, Adam L, et al. A transatlantic perspective on 20 emerging issues in biological engineering. Elife. 2017;6:e30247. doi:10.7554/eLife.30247
26. Webber BL, Raghu S, Edwards OR. Is CRISPR-based gene drive a biocontrol silver bullet or global conservation threat?. Proc Natl Acad Sci USA. 2015;112(34):10565-7. doi:10.1073/pnas.1514258112
27. Seager TP, Trump BD, Poinsatte-Jones K, Linkov I. Why life cycle assessment does not work for synthetic biology. Environ Sci Technol. 2017;51:5861-2. doi:10.1021/acs.est.7b01604
28. Esvelt KM, Gemmell NJ. Conservation demands safe gene drive. PLoS Biol. 2017;15(11):e2003850. doi:10.1371/journal.pbio.2003850
29. Esvelt K, Millett PD. Genome editing as a national security threat. Revue scientifique et technique (International Office of Epizootics). 2017;36(2):459-65. doi:10.20506/rst.36.2.2666
30. Sharma A, Gupta G, Ahmad T, Krishan K, Kaur B. Next generation agents (synthetic agents): Emerging threats and challenges in detection, protection, and decontamination. In Handbook on biological warfare preparedness. Chapter 12. 2020. pp. 217-256.
31. Hummel S, Burpo FJ, Hershfield J, Kick A, O'Donovan KJ, Barnhill J. A new age of bioterror: anticipating exploitation of tunable viral agents. CTC Sentinel. 2022r;15(4):1-6.
32. Juling D. Future Bioterror and Biowarfare Threats for NATO's Armed Forces until 2030. Journal of Advanced Military Studies. 2023;14.
33. Evans SW, Beal J, Berger K, Bleijs DA, Cagnetti A, Ceroni F, et al. Embrace experimentation in biosecurity governance. Science. 2020;368(6487):138-40. doi:10.1126/science.aba2932
34. Kuiken T. Governance: Learn from DIY biologists. Nature. 2016;531(7593):167-8. doi:10.1038/531167a
35. Novossiolova T, Kuiken T, DeCoste J, Henry L, Malsch I, Merad M, et al. Addressing emerging synthetic biology threats: The role of education and outreach in fostering effective bottom-up grassroots governance. Emerging Threats of synthetic biology and biotechnology: addressing security and resilience issues. 2021:81-102. doi:10.1007/978-94-024-2086-9_6
36. Trump BD, Siharulidze G, Cummings CL. Synthetic biology and risk regulation: the case of Singapore. In Synthetic Biology 2020: Frontiers in Risk Analysis and Governance. Cham: Springer International Publishing. 2019. pp. 297-312. doi:10.1007/978-3-030-27264-7_13
37. Linkov I, Keenan JM, Trump BD, editors. COVID-19: systemic risk and resilience. Springer International Publishing; 2021.
38. Evans NG, Selgelid MJ. Biosecurity and open-source biology: the promise and peril of distributed synthetic biological technologies. Sci Eng Ethics. 2015;21(4):1065-83. doi:10.1007/s11948-014-9591-3
39. Wein LM, Liu Y. Analyzing a bioterror attack on the food supply: the case of botulinum toxin in milk. Proc Natl Acad Sci USA. 2005;102(28):9984-9. doi:10.1073/pnas.0408526102
40. Shinwari ZK, Khalil AT, Nasim A. Natural or deliberate outbreak in Pakistan: how to prevent or detect and trace its origin: biosecurity, surveillance, forensics. Arch Immunol Ther Exp. 2014;62(4):263-75. doi:10.1007/s00005-014-0298-6
41. Faezi S, Chhetri RR, Malawade AV, Chaput JC, Grover W, Brisk P, et al. Oligo-Snoop: A Non-Invasive Side Channel Attack Against DNA Synthesis Machines. Network and Distributed Systems Security (NDSS) Symposium. 2019.
42. Zilinskas RA. A brief history of biological weapons programmes and the use of animal pathogens as biological warfare agents. Revue scientifique et technique (International Office of Epizootics). 2017;36(2):415-22. doi:10.20506/rst.36.2.2662
43. Anand M. A systems approach to agricultural biosecurity. Health Secur. 2018;16(1):58-68. doi:10.1089/hs.2017.0035
44. Yeh JY, Lee JH, Park JY, Cho YS, Cho IS. Countering the Livestock-Targeted Bioterrorism Threat and Responding with an Animal Health Safeguarding System. Transbound Emerg Dis. 2013;60(4):289-97. doi:10.1111/j.1865-1682.2012.01349.x
45. Mehlman MJ, Conlon RA, Pearlman A. Governing nonconventional genetic experimentation. J Law and the

Biosci. 2023;10(1):lsad003.
46. Patrick S, Barton J. Mitigating Risks from Gene Editing and Synthetic Biology: Global Governance Priorities. Carnegie Endowment for International Peace. 2024.
47. Trump BD, Florin MV, Perkins E, Linkov I. Emerging Threats of Synthetic Biology and Biotechnology. Chapter 1. Biosecurity for Synthetic Biology and Emerging Biotechnologies: Critical Challenges for Governance. Published in Cooperation with NATO Emerging Security Challenges Division. 2021.
48. Gillum D, Carrera LA, Mendoza IA, Bates P, Bowens D, Jetson Z, et al. The 2017 Arizona biosecurity workshop: an open dialogue about biosecurity. Appl Biosaf. 2018;23(4):233-41. doi:10.1177/1535676018781854
49. Oliver A. Behavioral economics and the public acceptance of synthetic biology. Hastings Cent Rep. 2018;48:S50-5. doi:10.1002/hast.819
50. Ritterson R, Kingston L, Fleming AE, Lauer E, Dettmann RA, Casagrande R. A call for a national agency for biorisk management. Health Secur. 2022;20(2):187-91. doi:10.1089/hs.2021.0163
51. De Bьrca G, Keohane RO, Sabel C. Global experimentalist governance. Br J Political Sci. 2014;44(3): 477-86.
52. Sabel CF, Zeitlin J. Learning from difference: The new architecture of experimentalist governance in the EU. Eur Law J. 2008;14(3):271-327. doi:10.1111/j.1468-0386.2008.00415.x
53. Sabel CF, Zeitlin J. Experimentalism in the EU: Common ground and persistent differences. Regul Gov. 2012; 6(3):410-26. doi:10.1111/j.1748-5991.2012.01157.x
54. Eckert S, Burzel TA. Experimentalist governance: An introduction. Regul Gov. 2012;6(3):371-7. doi:10.1111/j.1748-5991.2012.01163.x
55. Sabel CF, Victor DG. Governing global problems under uncertainty: making bottom-up climate policy work. Clim Chang. 2017;144(1):15-27. doi:10.1007/s10584-015-1507-y
56. National Research Council. Committee on Risk Perception and Communication, Improving Risk Communication; National Academy: Washington, DC, USA. 1989. pp. 2.
57. Littlewood J. Managing the Biological Weapons Problem: From the Individual to the International. August 2004. Available from: http://www.blixassociates.com/wp-content/uploads/2011/03/no14.pdf (accessed 30 September 2021).
58. Rhodes RA. The new governance: governing without government. Political Stud. 1996;44(4):652-67. doi:10.1111/j.1467-9248.1996.tb01747.x
59. Barben D, Fisher E, Selin C, Guston DH. Anticipatory Governance of Nanotechnology: Foresight, Engagement, and Integration. In The Handbook of Science and Technology Studies, 3rd ed, Hackett EJ, Amsterdamska O, Lynch M, Wajcman J. Eds MIT Press: Cambridge UK. 2007. pp. 979–1000.
60. Stoker G. Governance as theory: five propositions. Int Soc Sci J. 1998;50(155):17-28.
61. Tucker JB. For Case Studies of Historical Incidents of Bioterrorism. In Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons. Tucker JB, Ed MIT Press: Cambridge MA USA. 2000. pp. 13–17.
62. National Science Advisory Board for Biosecurity. Enhancing Responsible Science Considerations for the Development and Dissemination of Codes of Conduct for Dual Use Research. 2010. Available from: https://osp.od.nih.gov/biotechnology/national-science-advisory-board-for-biosecurity-nsabb/#reports_recommendations (accessed 20 September 2021).
63. Caruso D. Synthetic Biology: An Overview and Recommendations for Anticipating and Addressing Emerging Risks. Center for American Progress Press: Washington DC USA. 2008. pp. 10.
64. Bansak KC, Tucker JB. The Governance of Emerging Dual-Use Technologies. in Tucker. J.B. (ed.): Innovation, dual use, and security: Managing the risks of emerging biological and chemical technologies, Cambridge, Mass: MIT Press. 2012;305–339.
65. Xue Y, Yu H, Qin G. Towards good governance on dual-use biotechnology for global sustainable development. Sustainability. 2021;13(24):14056. doi:10.3390/su132414056