Redefining National and International Bioweapons Regulations in the Synthetic Biology and Digital Age

By
Ada Özgirin, Mohamed Soufi & Youssef Abdelmaksoud

Ada Özgirin | University of Paris Saclay - Evry | Home Country: Turkey

Mohamed Soufi | Independent Freelance Science Writer | Home Country: United States

Youssef Abdelmaksoud | French National Institute of Health and Medical Research (INSERM) | Home Country: Egypt

Executive Summary

Biological warfare has long been a threat, and modern advancements have allowed the tools for the development of biological weapons to become more accessible and harder to monitor. Nearly fifty years after the Biological Weapons Convention (BWC) was established, biology and related technologies are advancing at an exponentially increasing rate. Synthetic Biology, AI-assisted design, and automated lab tools allow cheaper and more accessible science, easing access to non-state actors, which complicate long-standing approaches for their regulation. This exposes gaps in existing frameworks in international governance and the BWC, and points to the need to update the original definitions and implementation mechanisms.

We suggest an updated definition retaining the core of the BWC's definition while expanding it to address new methods for bioweapons production and use. Without responding to these advancements and possible risks in time, existing frameworks risk falling behind the speed and scale of technology. Therefore, to meet the challenges of the future, we recommend four key actions.

1. **Strengthen global biosecurity governance** by updating legal protocols and establishing an independent implementation body.
2. **Modernise threat evaluation and regulation**, as advancements in both software and hardware aiding biological engineering lower the barrier to weaponize biology that current regulatory mechanisms are not equipped to address.
3. **Increase investments into biosecurity research and infrastructure** to enhance safety and scientific progress. This is necessary to develop potential countermeasures for future threats and improve the foundational systems for making biology safer to work with.
4. **Build a strong foundation for managing future risks.** This is possible through investing in biosecurity as a profession and increasing bioliteracy among the public.

The exponentially advancing pace of biotechnology means the world can no longer rely on outdated systems of biosecurity to keep us safe. Historically reactive responses must be replaced with proactive approaches.

Background

Using biology in warfare predates modern science, dating back to the 14th century BC when Hittites introduced tularemia-infected rams into enemy villages[1]. A more recent example includes the deliberate transmission of smallpox during the Seven Years' War. Following the extensive use of chemical weapons in World War I, the Geneva Protocol of 1925 prohibited the use of chemical weapons in conflict, as well as the "use of bacteriological methods of warfare"[2], but provided no detailed definition for biological weapons. Moreover, it did not prohibit their development or stockpiling. This led to the continuation and initiation of programs such as Imperial Japan's biological-warfare unit during World War II, which is estimated to have killed at least 200,000 civilians[3].

The Biological Weapons Convention (BWC) [4] entered into force in 1975 as the first international agreement prohibiting the development, production, acquisition, transfer, and use of biological weapons and their delivery. It didn't specify characteristics or origin of the biological agents, opting for a general ban on a "general purpose criterion" and focusing on the intent of development and use. This framing allows the BWC to remain applicable to future scientific developments. However, much of the global response to biological threats is reactive rather than proactive: the BWC was negotiated in response to the cold war bioweapons programs.

In the same year the BWC went into force, the Asilomar Conference set the first guidelines on recombinant DNA. Participants agreed to ban large-scale cultures of recombinant organisms and any DNA recombination from highly pathogenic organisms and toxic genes [5]. At the Spirit of

Asilomar conference 50 years later, 27 treatises were issued, including one reaffirming commitment to the BWC charter and another banning mirror-life research[6,7].

Today, decades after the Geneva protocol and the BWC, the biothreat landscape has shifted dramatically. Rapid advances in digital and biological technology are reshaping not only what constitutes a weapon but also who might create and deploy one [8]. Tools such as CRISPR-Cas9, AI-assisted protein modeling, whole genome design, immunogenicity predictions, along with growing access to cloud labs and DNA synthesis make it possible to modify existing organisms and construct new ones. These advances expand the means and potential impact of bioweapons, blur the line between natural and synthetic threats, and lower the barrier for non-state actors to access knowledge and capability.

In light of these changes, the principles of the BWC become more relevant than ever, but we need a new definition that reflects the shifted boundaries of what constitutes a biological weapon.

We define biological weapons as:

> ***any replicating or biologically active agent, product, or means of delivery—whatever their origin, natural, modified, or fully synthetic—that is deliberately designed, developed, produced, acquired, stockpiled, or used to harm, disrupt, or exploit biological systems for hostile purposes.***

This updated definition retains the core emphasis on intent while broadening its reach to encompass threats made possible by modern biotechnology.

Discussion

A report from 2003 from the CIA[9] highlighted that "traditional intelligence for monitoring WMD development could prove inadequate to deal with the threat from advanced biological weapons"; a concern amplified today by decentralized biotechnology. Technologies that once required nation-state resources are now accessible in community labs, high schools, and even DIY biology settings. Benchtop DNA synthesizers are available commercially for around $35,500. High-throughput sequencing is similarly affordable, with sequencer models starting around $300 [10]. Free and anonymous genetic design and cloning software,like Benchling and AlphaFold, along with open-source databases of complete pathogen genomes, like NCBI, are freely accessible online. In 2024, this led to the scientific community demanding standardized screening practices and repositories for synthetic DNA sequences, including oversight of benchtop nucleic acid synthesizers[11]. While commercial DNA synthesis providers generally screen for pathogenic sequences, enforcement varies widely. In total, technology advancements significantly reduce technical and financial barriers, broadening the potential pool of actors capable of developing novel biological agents.

Engineering synthetic organisms or modifying pathogens presents new detection, attribution, regulatory, and response challenges. Future biological threats may be subtle, designed to evade the immune system, delay symptoms, or evade other sensors. Current screening and oversight systems are outdated to catch engineered agents, leaving gaps that bad actors could exploit to directly create bioweapons or to indirectly use biology to aid conventional arms production.

The continually evolving nature of biological threats demands not only the ability to identify and respond to threats, but also the legal and normative frameworks intended to prevent their use. The BWC, while conceptually flexible, was negotiated before synthetic biology, and its mechanisms reflect that. Unlike the Chemical Weapons Convention (CWC) and the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), the BWC relies on voluntary declarations and confidence-building measures. Without a verification mechanism or frequent inspections, the ability to respond to developing risks depends on voluntary collaboration and political will. As synthetic biology advances, its deterrent power becomes increasingly ineffective unless the BWC gains stronger, modernized enforcement tools.

Biosecurity surveillance also typically depends on voluntary compliance. For example, U.S. FDA-approved environmental releases of biological agents require no mandatory follow-up reporting. Without standardized evaluation frameworks and mandatory traceability, accountability remains limited, increasing risks of negligence or misuse.

While UN Security Council Resolution 1540 imposes obligations on states to prevent non-state actors from acquiring biological weapons, it offers limited guidance on how to address dual-use research, distributed technologies, or the governance of digital genetic information. Current frameworks focus largely on controlling materials and equipment, but as the technology shifts into the digital and informational domains, new forms of oversight—such as an implementation arm of the BWC—may be required.

Additionally, the combination of low-cost, powerful biotechnologies with dispersed international regulation increases the possibility of a biological weapons race, which might be initiated not just by governments but also by lone actors, ideologically motivated groups, and irresponsible scientists. International security may become more unstable if the threshold for the development of bioweapons continues to decrease and multilateral action remains reactive and slow.

Competition among states and non-state actors can drive innovation, but when taken to extremes, can significantly threaten biosecurity and undermine the BWC. As Senator Todd Young, chair of the US National Security Commission on Emerging Biotechnology, said, “One thing we did not contemplate—and will not contemplate *unless the American people change their views on this*—is creating bioweapons. This is something the United States does not and will not do—but China, or others, might.” The caveat for “unless the American people change their views on this” is worrying and highlights the danger of how increased competition and disregard for international agreements could rapidly erode consensus and compliance with the BWC.

The COVID-19 pandemic exposed serious gaps in bioliteracy as misinformation spread. Misinformation and resistance to vaccines and masks cost thousands of lives. Although the lab-leak debates can draw attention to real dual-use risks, the controversy has largely affected trust in science and stoked fear of biological research[11,12]. Much of the speculation stoked resentment toward China and revived unfounded bioweapon rumors, fears that could even spur some governments to pursue their own programs. When citizens cannot distinguish genuine biological threats from alarmist rhetoric, society becomes vulnerable to both danger and demagoguery.

Ultimately, the definition of biological weapons evolves alongside biotechnology, and so too must the mechanisms to prevent their development and use. A more proactive strategy is required. We recommend the gap between scientific innovation and global governance be bridged with the support of policies covered in the recommendations section.

Recommendations

1. Reforming Global Biosecurity Governance

The BWC should mirror the CWC with additional protocols and an implementation body to monitor compliance, facilitate inspections, and assess new biotechnologies. The UN Security Council, which is responsible over BWC disputes, should leverage Resolution 1540[13] and its Chapter VII mandate to counter non-state threats by creating frameworks for early warning, coordinating biothreat responses, and strengthening BWC institutions. Moreover, governments should proactively regulate high-risk biotechnologies at the software and hardware level, invest in biosecurity research, and build a bioliterate workforce and population. Regular treaty reviews, a science advisory board, and compliance-monitoring mechanisms will ensure the BWC evolves alongside scientific innovation.

Biosecurity governance should adopt an adaptive, experimental mindset[14], allowing policies to adjust based on new evidence. However, modern bioweapons remain largely hypothetical, so we lack clear evidence to guide policy. Useful outcome metrics are difficult to define, so we propose rigorous red-teaming to assess risks. Nonetheless, gathering real-world evidence on policy remains critical, and demands transparent national and international data sharing that unites state and independent groups, like the Integrated Biosecurity Index and Global Health Security Index. This analysis should define and regularly update the BSL-3+ facilities in each state, in line with Recommendation 2 on modernizing threat evaluation.

We recommend that the BWC address both direct violations and negligence with economic and collaborative sanctions against countries, institutions, and individuals. Legal norms and article IV of the BWC hold states accountable for preventing all harmful activities within their borders. Individual accountability, coupled with rewards and robust whistleblower protections, can also promote transparency and proactive reporting.

2. Modernizing Threat Evaluation and Regulation

To match rapid biotechnology advances, we propose a graduated classification system for dual-use biological agents, modeled after U.S. Biosafety Levels (BSL). The BWC's implementation body should standardize biosecurity measures and mutual auditing processes across member states. The proposed standards should determine audit frequencies based on a biological agent's estimated time to weaponization as determined by experts.

Biological engineering combines physical "hardware" (cells, nucleic acids, proteins) using "software" (design tools, models). Today's synthetic-biology workflow runs on tools that span basic cloning suites (Benchling, SnapGene) to AI-enabled design engines (Cello, Evo, AlphaFold). Because software regulation is digital, it can be automated, centrally enforced, and updated quickly, forcing would-be bioweaponeers onto slower, costlier, and riskier unprincipled methods[15]. We therefore recommend embedding safety checks directly in synthetic biology software: monitor user inputs, require intent clarifications from users, and automatically flag, block, or report requests that match biothreat criteria. Access to any software handling BSL-3+ work should also require verified log-in with a government-issued or institutional ID. The BWC, national regulators, and biosecurity experts should jointly define and implement these rules.

Hardware regulation remains essential, but relies on costly and decentralized enforcement[15]. Some measures should be put in place, such as export controls, tracking of purchases of dual-use equipment, and equipping DNA synthesizers with a built-in sequence-screening software. While these measures could be bypassed by a black market or expert users, they're better than not having any hardware safeguards.

Table 1: A proposed updated BSL system that builds on existing U.S. Biosafety Levels, and takes into account how scientific and technological innovations might enable the creation of new threats beyond normal regulated agents as well as estimated times for an agent's weaponization. A scientific advisory should continually monitor and update the classifications of agents.

BSL Level	Explanation	Example Agents	Estimated people-years of development for agent to become weaponized
BSL-1	Work with well-characterized agents not known to cause disease in healthy adults. Open bench work; basic microbiological practices; sink for hand-washing; Register with a biosecurity officer, but generally this work can go unsupervised.	*Escherichia coli* K-12 *Bacillus subtilis* *Cell-Free Translation Reaction* *GFP plasmid* *Collagen Protein* *DNA delivery into lab-grade bacteria (electroporation, heat shock)*	*<5 people-years*
BSL-2	Moderate-risk agents that pose a hazard if mishandled. Limited lab access; use of Biosafety Cabinet (Class II) for procedures likely to generate aerosols; Must have access to equipment that can decontaminate laboratory waste; Basic personal protective equipment (PPE); One biosecurity officer can supervise many BSL 2 labs.	*Salmonella enterica* *Hepatitis B virus* *Staphylococcus aureus* *Synthetic Cells that can replicate* *Genetic circuits for human cells* *DNA delivery into human cells* *Horizontal Gene Transfer between bacteria*	*<1 year*
BSL-3	Agents that may cause serious or potentially lethal disease. Controlled access; directional airflow (negative pressure); sealed penetrations; all work must be done in biosafety cabinets; More extensive PPE; Each lab should appoint a dedicated biosecurity officer to coordinate with a national BWC implementation body.	*Mycobacterium tuberculosis* *SARS-CoV-2* *Francisella tularensis* *Protein toxins/plasmid encoding protein toxin* *Pathogenic plasmids for lab grade bacteria* *Enhanced DNA delivery into key human organs (brain, lungs, heart, liver, kidneys)*	*<6 months*
BSL-4	Dangerous/exotic agents with high risk of aerosol-transmitted infection and no known treatment or vaccine. Separate building or isolated zone; full-body PPE, air-supplied positive-pressure suit or Class III cabinet; Each lab should appoint multiple dedicated biosecurity officers and register with the BWC.	*Ebola virus* *Marburg virus* *Lassa virus* *CAR-T circuits targeting healthy human cells* *Lethal virus aerosols* *Lethal fungi spores*	*<1 month*

3. Investing in Biosecurity Research

We recommend significant investments in biosecurity research from governments and their defence organizations, universities, and the private sector to develop proactive technological countermeasures against emerging biological threats (Figure 1).

Investment into the development of rapid, precise, and affordable sensors for hazardous biological agents would allow for routine monitoring, including for air-borne pathogens[16]. This could deliver the development of a global map displaying the spread of emerging and existing pathogens spread, akin to a weather forecast. Existing examples of such tools were developed during COVID-19[17]. Those investments will enhance national and international resilience and preparedness against biosecurity threats, especially when integrated with improved data collection and sharing outlined in the previous recommendations. We also recommend encouraging research into genetic attributions[18], and mandate stricter rules for environmental release of biological agents, requiring them to follow a phased approach similar to clinical trials.

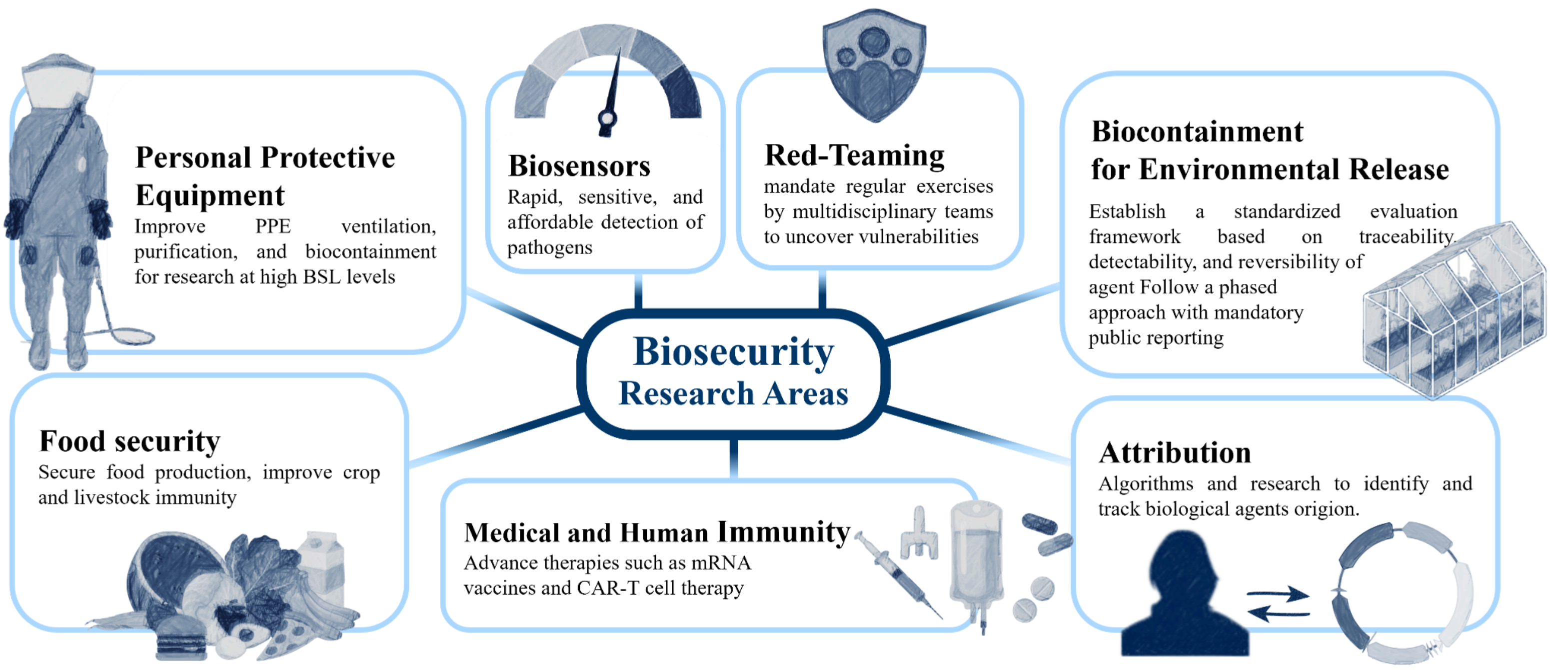

Figure 1: Key biosecurity research areas include biocontainment strategies for phased environmental releases, sandboxing, pathogen sensors for air and water, attribution methods such as surface proteins (similar to MHC domains) or DNA barcodes, medicine and human immunity, food security, personal protective equipment, and red-teaming to identify vulnerabilities in our defenses.

Regularly mandated red-teaming exercises are crucial for identifying and mitigating vulnerabilities. Further investments should target crop protection, secured food production methods (e.g., lab-grown meat), vaccines, therapeutics, and protective gear. All biosecurity research outcomes must remain transparent and publicly accessible to maintain accountability and international cooperation.

4. Investing in Biosecurity Professionals and Bioliterate Citizens

We recommend increasing investment in bioliteracy and promoting biosecurity as a professional field, similar to cybersecurity. Clear pathways and degree programs should be established for students pursuing biosecurity careers. Globally recognized credentials in biosecurity should become standard, gradually requiring credentialed staff at life-science facilities[19]. Opportunities should extend beyond research and policy to sectors like transportation, agriculture, health, and manufacturing.

Building broad bioliteracy is equally important. An informed public will be less likely to tolerate bioweapon development and more likely to engage meaningfully in biosecurity discussions. High school curricula should incorporate biosecurity topics, including historical incidents.

University biology programs should include mandatory biosecurity coursework. Professional biologists and bioengineers must stay informed of BWC developments, cultivating a vigilant biosecurity community. However, education programs must carefully avoid creating infohazards by teaching awareness without disclosing detailed misuse pathways.

Regular opinion and awareness polls will assess bioliteracy initiatives' effectiveness. A resilient biosecurity culture requires sustained public investment, interdisciplinary training, and international collaboration. Developing these components will encourage proactive global preparedness against future biological threats at the grassroots level.

Conclusions

Our analysis highlights the evolution of potential biological weapons driven by advancements in synthetic biology and artificial intelligence. Historically, biological warfare leveraged naturally occurring pathogens, but modern biotechnology enable the creation of entirely synthetic organisms and engineered biological threats. This has created gaps in international frameworks, notably the BWC, necessitating an updated definition and clear implementation mechanisms.

We propose an expanded definition of biological weapons that maintains the BWC's core intent-based criterion and explicitly addresses modern biotechnology advances. This updated definition is critical for clarifying current threats, assessing risks accurately, and enforcing accountability.

To address these evolving threats, we recommend four priority actions for the international community:

- First is strengthening the global biosecurity governance. This can be implemented through updated legal protocols and establishing an independent implementation body for coordinating international oversight, enforcing accountability, and guiding states and institutions.
- Secondly, there is a need to modernise threat evaluation and regulation. Regulation should incorporate both technical understanding and risk assessment, continuously evolving with new technology.
- Thirdly, we call for investments in biosecurity research to develop potential countermeasures for future threats.
- Lastly, there is a need to build biosecurity workforce and bioliterate population. Training experts and raising awareness will greatly encourage cooperation and international trust.

Regardless of the specifics, biosecurity governance should embrace an adaptive, evidence-driven approach. Because modern bioweapons remain largely theoretical and documented violations are rare, clear metrics to evaluate policy success remain elusive. Therefore, we propose rigorous red-teaming exercises and active, transparent data-sharing among nations to generate meaningful data and refine policy accordingly.
Preventing bioweapons is the central aim, but the same recommendations yield benefits far beyond biosecurity. A bioliterate society paired with stronger international governance can spark the kind of global collaboration we glimpsed during COVID-19. Biosecurity research will also bolster food security, drive medical breakthroughs, and improve sensors for all devices. In short, these policies not only guard against emerging threats but also accelerate science advances, educate the public, and unite nations.

Appendix

List of experts consulted for the paper.

We thank the following experts for their time and consultation:

- **André de Hoogh** - Associate Professor in International Law, University of Groningen
- **Ariel Lindner** - Director of Research at INSERM, Board member at the International Bioethics Committee (UNESCO), and iGEM Foundation
- **Aurelia Attal-Juncqua** - Biosecurity Policy Researcher, RAND Corporation
- **Leon Elcock** - b.next Biomanufacturing Associate, Spirit of Asilomar Next Generation Leader
- **Liyam Chitayat** - Council on Strategic Risks Research Fellow, Spirit of Asilomar Next Generation Leader, MIT Ph.D

Abbreviations

AI	Artificial Intelligence
BSL	Biosafety Level
BWC	Biological Weapons Convention
CAR-T	Chimeric Antigen Receptor T-cell
COVID-19	Coronavirus Disease
CRISPR-Cas9	Clustered Regularly Interspaced Short Palindromic Repeats - CRISPR associated protein 9
CWC	Chemical Weapons Convention
FDA	Food and Drug Administration
MHC	Major Histocompatibility Complex
NCBI	National Center for Biotechnology Information
NPT	Treaty on the Non-Proliferation of Nuclear Weapons
PPE	Personal Protective Equipment
UN	United Nations

References

1. Arizti Sanz, Jon, Garrett Dunlap, Nicholas Nolan, and Colin O'Leary. 2022. "Biosecurity Risks and Governance in the Age of Synthetic Biology." *MIT Science Policy Review* 3 (August):136–42.
2. Baker, David, and George Church. 2024. "Protein Design Meets Biosecurity." *Science (New York, N.Y.)* 383 (6681): 349.
3. Berg, P., D. Baltimore, S. Brenner, R. O. Roblin, and M. F. Singer. 1975. "Summary Statement of the Asilomar Conference on Recombinant DNA Molecules." *Proceedings of the National Academy of Sciences of the United States of America* 72 (6). https://doi.org/10.1073/pnas.72.6.1981.
4. Campos, Luis A. 2024. "A Little Care before We Leap." *Science (New York, N.Y.)* 385 (6716): 1424–25.
5. Chung, Christine. 2021. "Meet the Winners of the Genetic Engineering Attribution Challenge." DrivenData Labs. January 26, 2021.

https://www.drivendata.co/blog/genetic-engineering-attribution-winners.
6. Cologna, Viktoria, Niels G. Mede, Sebastian Berger, John Besley, Cameron Brick, Marina Joubert, Edward W. Maibach, et al. 2025. “Trust in Scientists and Their Role in Society across 68 Countries.” *Nature Human Behaviour* 9 (4): 713–30.
7. Evans, Sam Weiss, Jacob Beal, Kavita Berger, Diederik A. Bleijs, Alessia Cagnetti, Francesca Ceroni, Gerald L. Epstein, et al. 2020. “Embrace Experimentation in Biosecurity Governance.” *Science (New York, N.Y.)* 368 (6487): 138–40.
8. Kumar, Joshin, Meng Xu, Yuezhi August Li, Shu-Wen You, Brookelyn M. Doherty, Woodrow D. Gardiner, John R. Cirrito, et al. 2025. “Capacitive Biosensor for Rapid Detection of Avian (H5N1) Influenza and in Aerosols.” *ACS Sensors* 10 (5): 3381–89.
9. Lee, Ying-Chiang Jeffrey, and Barbara Del Castello. 2024. “Robust Biosecurity Measures Should Be Standardized at Scientific Cloud Labs.” RAND Corporation. November 8, 2024. https://www.rand.org/pubs/commentary/2024/11/robust-biosecurity-measures-should-be-standardized.html.
10. Mavragani, Amaryllis, and Konstantinos Gkillas. 2020. “COVID-19 Predictability in the United States Using Google Trends Time Series.” *Scientific Reports* 10 (1): 20693.
11. Moritz, Rebecca L., Kavita M. Berger, Barbara R. Owen, and David R. Gillum. 2020. “Promoting Biosecurity by Professionalizing Biosecurity.” *Science*, February. https://doi.org/10.1126/science.aba0376.
12. NYT. 1995. “Unmasking Horror -- A Special Report.; Japan Confronting Gruesome War Atrocity.” *The New York Times*, March 17, 1995. https://www.nytimes.com/1995/03/17/world/unmasking-horror-a-special-report-japan-confronting-gruesome-war-atrocity.html.
13. Reid, Blake E. 2016. “Regulating Software When Everything Has Software.” *The George Washington Law Review*. https://www.gwlr.org/wp-content/uploads/2016/11/84-Geo.-Wash.-L.-Rev.-1672.pdf.
14. “Rethinking Biosecurity in the 21st Century: An Enhanced Role for Civil Society.” 2023. *Journal of Biosafety and Biosecurity* 5 (3): 100–106.
15. Straits Research. n.d. “DNA Synthesizer Market Size, Growth, Trends & Demand Report by 2033.” Accessed July 13, 2025. https://straitsresearch.com/report/dna-synthesizer-market.
16. The Office of Transnational Issues. n.d. “The Darker Bioweapons Future.” Accessed July 13, 2025. https://irp.fas.org/cia/product/bw1103.pdf.
17. “‘The Spirit of Asilomar and the Future of Biotechnology’ Summit.” n.d. “The Spirit of Asilomar and the Future of Biotechnology” Summit. Accessed July 13, 2025. https://www.spiritofasilomar.org/.
18. Trevisanato, Siro Igino. 2007. “The ‘Hittite Plague’, an Epidemic of Tularemia and the First Record of Biological Warfare.” *Medical Hypotheses* 69 (6): 1371–74.
19. UN. Security Council (59th year : 2004). n.d. *Resolution 1540 (2004) / Adopted by the Security Council at Its 4956th Meeting, on 28 April 2004*. UN,. Accessed July 13, 2025.