

WHY PUBLIC TRUST IS THE CORNERSTONE OF BIOSECURITY

BY CHARLOTTE ESLER

Charlotte Esler *(charlotte.v.esler@gmail.com) works in innovation and emerging technologies at NATO. She previously was the COO of a deep technology spinout and worked in finance in Europe and Asia. She has a Master in Public Policy from Harvard Kennedy School, a Master of Business Administration from the University of Cambridge, and a Bachelor's degree in Politics from SOAS University of London. She is a member of the 2023 cohort of Pacific Forum Young Leaders. The views expressed here are hers alone.*

Biorisks are poorly understood and therefore inadequately mitigated. Advances in biotechnology, breakthroughs in enabling technical areas like artificial intelligence, and intensifying geopolitics increase the urgency of developing a coherent risk mitigation framework. The fact that biosecurity does not neatly fall under the exclusive remit of a single government authority makes cross-functional government approaches under a clear and accountable authority structure highly desirable for effective risk mitigation. Public trust is also vital for policymaking legitimacy. Analytically rigorous government risk assessments based on biosurveillance data alongside appropriate levels of clear public disclosure are key to building the necessary public confidence in biosecurity policy.

The Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory (LLNL) convened its biennial biosecurity workshop in March 2026. The workshop brought together experts from across the United States' and allies' biosecurity landscape. This article synthesizes and builds on aspects of these discussions to explain why coherent responses to current and emerging biosecurity risks should be grounded in the principle of public trust, which is a cornerstone of legitimacy and effective administration in all democracies. While this article is inspired by the dialogue at CGSR, the perspectives expressed here are not those of that or any other organization.

To tackle a problem, you first must understand it

Various factors make biorisks hard to understand and effectively mitigate. Biorisks are diverse and span biological weapons development and use, accidental laboratory leaks, or natural outbreaks. Potential threat profiles are also varied and might include nation states with different degrees of resource and sophistication, terrorist groups, criminals, and negligent lab workers or poorly maintained facilities. Risk analysis is hindered by the inherent secrecy of biological weapons development, which is illegal under the Biological Weapons Convention (BWC).

This is compounded by the fact that it can be difficult to distinguish legitimate biotechnology innovation from illegal work, and to attribute dangerous biological agents to their source. While many of these issues are not exceptional to biotechnology—attribution issues pervade the cybersecurity world, for instance, and all dual-use technologies can be used for both positive and adversarial ends—the exact permutation of these risks for biotechnology development is unique and biosecurity therefore requires specific policy consideration. This need is made more acute by the fact that while biological agents are often grouped alongside nuclear risks as part of a CBRN/WMD (Chemical, Biological, Radiological and Nuclear/Weapons of Mass Destruction) nexus, they are qualitatively different given the potential for more widespread development and since they might have a natural origin and therefore have distinct deterrence and counterproliferation considerations.

The biorisk surface is also expanding. AI advances make the ability to develop novel pathogens more accessible, while the dark web means that dangerous substances could, at least in theory, be procured from anywhere in the world. The increasing number of high Biosafety Level (BSL) laboratories raises the difficulty of establishing whether safety best practices have been maintained, increasing the potential for accidental leaks.

In response, governments should look to develop a more complete and dynamic understanding of the biorisk picture from which they can derive mitigating policies and build public confidence in these measures over time through appropriate disclosure and clear communication. This approach is necessary to maximize the

benefits of biotechnology breakthroughs, which have the potential to save and improve the lives of millions and to enable the responsible development of adjacent technologies like artificial intelligence whilst minimizing the scope for technological misuse.

The need for public trust

Effective biosecurity policymaking relies on a coherent, multidisciplinary government response and public trust. Whole-of-society approaches are necessary to respond effectively to biological threats regardless of whether they are the result of an intentional attack, accidental laboratory leak, or natural occurrence. Scientific rigor alone, such as the existence of safe and effective vaccines for serious illnesses, is not enough to fully mitigate risks if public reservations about these treatments remain.

Multidisciplinary approaches are key to competent policy development

A prerequisite for trust building is increasing the attentiveness of key stakeholders to biological risks to develop the necessary cross-functional responses. The biological threat falls under the purview of various parts of the public sector, including defence and security communities and health and agriculture ministries.

Varied and broadening parts of the technology and health-related private sector, including start-ups, also play an important role in protecting public health. While these private sector actors may understand technical risk factors well (for instance, the obligation of responsible laboratory practices) they may under-appreciate the fact that they are developing dual-use technologies with potential defensive applications and therefore counterproliferation considerations.

Policymakers, meanwhile, may inadequately recognize the constraints that smaller companies face, including limited financial means and low awareness of government priorities. It is important therefore that all these communities not only participate in improving societal understandings of biological risks but also recognize that they have a crucial role in responding to them. This outcome is hampered by the tendency for intellectual siloing (defense can view biosecurity as a health issue and health officials can view biosecurity as a defense issue, for instance), and the fact that biological risks are often speculative future crises, meaning that policymakers, hospital administrators, and others have low incentive to develop proactive responses when they have more urgent issues to tackle.

While the buy-in of multiple stakeholders is necessary, inclusion without thoughtfully considering where the authority of one institution ends and another's begins has the potential to create conditions for buck-passing and impasse. It is therefore necessary to define the precise mandates of different government authorities and develop cross-functional organizations as necessary. It is also desirable for these organizations to coordinate their activities under the framework of a preeminent national strategy to maximize coherence and reduce the risk of inadvertent undermining and duplication.

Analytical rigor through biosurveillance

Biosurveillance is the real-time collection and characterization of biological data to detect biological threats using technologies like genetic sequencing and artificial intelligence. It can be used to establish baselines and monitor deviations that could suggest early signs of outbreak, such as increased over-the-counter pharmaceutical sales, or novel or highly dangerous pathogens in wastewater, air, or soil.

If developed with the appropriate data governance and proportionate usage safeguards in place, improved biosurveillance has the potential to create a more biosecure society by transforming understandings of biorisks, enabling shared understandings across government, and ensuring that policies are based in analytical rigor. It could be used to increase public trust in specific policy interventions through making the need for ordering more personal protective equipment (PPE), vaccinations, or other emergency mitigations explainable through certain data points crossing pre-determined thresholds.

It could also reduce the risk for under- or over-reaction to outbreaks and other biological events by making mitigations data-driven rather than about pre-empting hypothetical applications of potentially dangerous technologies. By enabling earlier detection of pathogens, biosurveillance in combination with artificial intelligence has the potential to improve countermeasure development, as well as hasten attribution over time. The collection and communication of high-quality data could also reduce disinformation and analytical bias regarding the spread of disease.

Conclusion

Public trust is paramount to effective legitimate policy execution in any democracy. Biorisks are hard to understand and do not fall under the aegis of any single government institution. Improving government's understanding of biorisks through biosurveillance and carefully defined government authorities can improve the quality of policy development. Clear public communication, supported by the analytical rigor provided by extensive and credible data, and appropriate transparency and accountability mechanisms can improve public trust in biosecurity policy.

The Pilot *commentaries and responses represent the views of the respective authors. Alternative viewpoints are always welcomed and encouraged. Please write to rob@pacforum.org for more information on how to contribute.*