Health Security
Volume 20, Number 2, 2022 Mary Ann Liebert, Inc.
DOI: 10.1089/hs.2021.0165

COMMENTARY

Next-Generation Biowarfare: Small in Scale, Sensational in Nature?

David Gisselsson

Keywords: Bioweapons, Dual use, Synthetic biology, Next-generation sequencing, Pandemic response, Information war

The character of biological warfare is currently undergoing a substantial change. This change derives from 2 parallel developments: one in society, the other in science. First, biological security threats are moving from the realm of weapons of mass destruction to the domain of information warfare, where small-scale, targeted attacks may still have a massive psychological impact. The COVID-19 pandemic has shown us how effectively fears of infection can close down societies, sow mistrust among allies, and create political turmoil. Future biological wars may use the same dynamics to inflict shock and confusion upon the enemy by the mere threat of mass casualties, thereby circumventing several previous limitations of biological warfare.[1,2] Second, rapid developments in the field of synthetic biology may broaden the repertoire of bioweapons, enabling tactical versatility and more precise attacks. Preparedness to defend against biological attacks must keep pace with these developments, taking into account not only defense against disinformation but also the need to rapidly mobilize resources at the frontline of molecular biology. Better preparedness calls for closer collaboration between frontline civilian scientists and national security establishments to build rapidly scalable networks of expertise and infrastructure for medical intelligence.

From Weapons of Mass Destruction to Weapons of Mass Disruption

In the 21st century, large-scale political conflicts will not be limited to armed struggles but will encompass all of society. Battles of psychological influence will escalate, while isolated kinetic warfare may become a rarity.[3] What is and what is not war will be increasingly difficult to say. What is the place for biological warfare in this future battle of the narratives, often occurring in the gray zone between peace and war?

The COVID-19 pandemic has taught us that the threat of a serious health crisis may have a severe impact on democratic nations.[4] Fears of a health crisis can tip an entire society into turmoil,[5] in turn opening several other vulnerabilities. For example, an outbreak of infectious disease can push people to work and live in the digital sphere where they will be sensitive to cyberattacks and technical breakdowns.[6,7] It is becoming clear that a biological attack, however small, may still reach effects at the strategic level by shifting the target for biological weapons away from military contingents toward the

David Gisselsson, MD, PhD, is a Senior Consultant and Professor, Division of Clinical Genetics, Department of Laboratory Medicine, Lund University, Lund, Sweden.

whole of society.[8] To achieve authenticity and deliver a sustained psychological effect, a limited attack may nevertheless require a foundation in real-world events of a shocking nature. Taking this into account, the strategic success of future biological attacks in gray zone conflicts depends on the extent to which they:

- Have a linked information war objective, including a broad set of possible aims, such as distracting from the suppression of opposition movements in the attacker's homeland or toppling the government of the target nation
- Trigger worries of massive spread, stressing the importance that the pathogen appears highly contagious, even if that is not the case
- Instigate fear of severe disease or death, suggesting that truly lethal agents may be used or that the young will be targeted in order to maximize fear; fear of infection could also limit in-depth scientific investigations as to the cause, mechanism, and origin of disease
- Prevent traceability back to the attacker, with clouded origins and deniability being used to sow fear for new outbreaks; an unknown origin is also useful for creating a sense of lost control in the target population, while inspiring conspiracy theories directed toward the target nation's institutions
- Maximize the element of surprise, to circumvent any countermeasures from the target nation; the element of surprise may not be limited to the time and location of an outbreak but may also include the use of exotic or synthetic biological agents and unexpected routes of delivery
- Be psychologically impactful, to deliver maximum effect on the media landscape; ways to achieve this may be to target public events with a high degree of media coverage or target public figures
- Be small-scale in factual nature, to avoid spreading pathogens back to the attacker and their allies; this effect may be achieved by counting on effective countermeasures from the target state or using sophisticated biotechnology

Circumventing the Obstacles of Past Biological Warfare

Due to its targeted mode of operation, future biological warfare in the gray zone may circumvent most of the obstacles that prevented bioweapons from reaching strategic-level effects in the past.[1,2,8]

First, large-scale production and deployment of biological agents may no longer be needed. Deployment on a massive scale to reach tactical effect on the battlefield used to require that weaponized agents were environmentally robust. They also had to be paired with a delivery system that could provide large-scale exposure.[1,2] This factor made it challenging to keep bioweapons programs secret and also demanded considerable infrastructure investments. In contrast, because even small outbreaks can now reach effects at the strategic level, future bioweapon production facilities can easily be nested in industrial or academic molecular biology laboratories as long as these facilities are not open to international scrutiny.[9]

Second, the armamentarium of biological warfare will broaden its repertoire of useful biological agents.[10] Most classic programs of biological warfare have been largely restricted to natural pathogens, with the efforts of the Soviet Union near its end a well-known exception.[11] This has limited the range of agents to a handful of pathogens, against which countermeasures could be extensively planned. This limitation, however, is now being offset on a grand scale by ongoing developments in biotechnology.[12] Infectious agents and animal cells can now be built from scratch in research laboratories.[13] Every year, the full genomes of more and more bacteria and viruses are sequenced and published. The biotech toolbox is increasing, not least with help from CRISPR/Cas9 technology, allowing us to change the DNA of living organisms, including pathogens.[14] The increasing capacity to navigate big data via machine learning could also make genetic manipulation of pathogens more effective.[15] The purpose of such manipulation could be wide-ranging and include obvious improvement of weapons capacity such as increased transmission rate and enhanced virulence, toxin production, or resistance to antibiotics or vaccines. However, manipulation may be even more far-reaching and include the introduction of mutations that allow a jump from animal to human host or nucleic acid sequences that code for peptides with subtle, nonlethal effects, such as mimicking common benign but incapacitating diseases. It may even be feasible to construct functions for delayed presentation of symptoms, allowing broad dissemination from the point of transmission, so that victims will seek medical care at an array of dispersed medical facilities. Such a multipronged attack would make quarantine and other efforts for a coordinated crisis response difficult.

Third, self-protection on a large scale may no longer be needed. The use of classic bioweapon pathogens has rested on the condition that they must be treatable or preventable for the troops of the attacker.[1,2] Keeping outbreaks small and targeted may circumvent this issue. Furthermore, using agents with a high lethality and morbidity would typically facilitate limitation because victims will die or be hospitalized in isolation before the pathogen has had time to infect a large number of people. Notably, the shock effect of a highly lethal, but easily containable pathogen can be enhanced by concomitant spread of a more benign and thus more transmissible variant of the same pathogen, from which the need for self-protection is not very high. Recent progress in synthetic biology may also radically facilitate the limitation of an outbreak. While debated as to its feasibility,

it cannot be excluded that the increasing availability of data on human genetic variation may allow specific targeting of individuals or specific ethnic groups based on their genotypes.[16] Specific genetic targeting methodology could also be useful for targeting crops or livestock, which are often nation/culture specific and relatively genetically homogenous. Other ways to limit an outbreak could be by engineering the DNA of a pathogen in ways that would restrict its replication to only a certain number of cycles or to certain environmental conditions.[17] As an additional safety mechanism, an attacker may prepare for large-scale vaccine production against the applied pathogen. The COVID-19 pandemic has shown that vaccines can be produced at a rapid pace. Ironically, if the attacker can escape attribution while providing a timely vaccine to the world, the attacker may also succeed in creating positive publicity for its side in a conflict.

The factors previously listed all contribute to dissolving friction points that previously made biological war difficult to operationalize. However, at least one factor remains that may keep its role as a deterrent against biological attacks: their moral reprehensibility, especially when directed against civilian targets. This deterrent may even be enhanced in a modern battle of the narratives. Pragmatically, this means that if a biological attack is ever planned, it is more important than ever to make sure that someone else, or no one at all, gets the blame. Sowing confusion as to the origin of an instigated disease outbreak could be key to strategic success.[18]

The Thickening Fog of Biological War

Carl von Clausewitz, the father of modern strategic military thinking, used the metaphoric fog of war to characterize the uncertainty and confusion surrounding battle.[19] Nowhere has this confusion been more prominent than in today's conflicts, with an increasing use of nonmilitary means of warfare, often difficult to discern from criminal activity, recreational hacking, or accidental events. Attribution—finding out who is behind biological attack—will probably be challenging in the future.[20] Some of the main reasons attribution will be challenging:

- The global financial biotech sector is growing rapidly, with many actors, large and small, having complicated ties to each other, to governments, and to academia.
- While information flows freely online, the trend toward open science makes it mandatory for scientists to deposit more and more data,[21,22] such as genome sequences in open archives, free for any bad actors to grab.
- Setting up new technology platforms is becoming less expensive every year, primarily because the costs of genome sequencing, DNA synthesis, data analysis, and data storage are going down. The capacity to create now lethal strains of pathogens are currently available at most major universities around the world.
- More and more sophisticated delivery systems increase the possibilities for covert action. New possibilities within the fields of nanotechnology and small autonomous vehicles may broaden the repertoire of vectors beyond what is available today.[23,24]
- The community of bad actors is increasing in complexity and is no longer limited to rogue nation states but also includes private security contractors, criminal groups, and terrorist groups, all of which may act in concert or in parallel.

That accountability and attribution can be made difficult by shifting bioweapons production from the government to the private sector is well illustrated by the South African apartheid-era Project Coast, where several private companies were used as cover for the production of biological and chemical agents.[25] Today's global economy, where international biotech companies are becoming increasingly connected with large academic research institutions and with government agencies, provides near-perfect conditions for actors who want to hide biological weapons development under the cover of innocent-looking (dual-use) biomedical research.[10] Notably, one may have to anticipate that future antagonists may be a blend of states and nonstate actors using biological threats to pursue agendas that may not even be political—similar to developments in the field of cybersecurity where bad actors are often nongovernmental and work for profit.

Future Biodefense Requires Increased Civil–Military Synergy

How should democratic societies best prepare for the bleak future outlined in this paper? Further work to improve compliance to the Biological Weapons Convention by better mechanisms for regulation of dual-use technology is laudable.[26] However, societies must look beyond traditional means of biodefense such as biosurveillance and stockpiling vaccines, drugs, and personal protective equipment. In a future where sophisticated biology will be combined with information warfare, medical intelligence will be critical[27] because (1) high-resolution and updated assessment of the biotechnological capacity among antagonists will be vital to deny attackers the element of surprise and (2) we will need frontline research expertise and infrastructure to produce solid data to counter disinformation. Finally, large-scale datasets on pathogens, such as their genome sequences, will prove vital for rapid production of countermeasures.

As a civilian health professional, I suggest that an updated biosecurity strategy for democratic societies should include at least:

- Information countermeasures that can defend against damaging narratives appearing alongside a biological

attack. Considering the inevitable polarity between freedom of speech and information campaigns, public messaging must be carefully performed, preferably leaning heavily on well-validated and updated medical data.

- Rapid deployment of next-generation sequencing technologies to genetically characterize emerging threats and facilitate attribution.[28] This requires scalable logistics for rapid and extensive sampling of the population, where field investigation teams are linked with first-class molecular biology facilities.
- Rapid postmortem investigations of deaths from suspected new biological threats. The purpose of this is not only to sample potential pathogens, but also to characterize how new agents injure and kill—knowledge that is critical for treating victims that are still alive.[29]
- Secure data transmission and storage, and computational capacity that can rapidly be scaled up to analyze vast amounts of biological data. This should include a rapid and secure system to funnel data to producers of vaccines and other countermeasures.
- A closer collaboration among government, the defense sector, healthcare providers, the commercial biotech sector, and medical research institutions. It would be advantageous to draft plans and financial contracts that regulate this collaboration in peacetime, to be activated later in times of crisis. In the recent launch of the European Health Emergency Preparedness and Response Authority, the civil–military axis in such collaborations is strikingly absent, at least according to open sources.[30]
- A constantly updated pool of expert scientists and healthcare professionals that can be pulled into service when required. This indicates the need for security-cleared civilian experts who are regularly trained to mobilize in times of crisis—essentially a core of academic reservists.

Finally, a word of warning: when entering a new era of increased preparedness, it is essential to maintain a balanced approach. A hypervigilance among government agencies toward biological threats can be a vulnerability in itself, carrying the risk that small natural outbreaks of benign pathogens will trigger massive lockdowns, which hamper other elements of defense, prove financially costly, and risk attenuating the response once a real threat emerges. Finding out fast and with high precision what exactly caused a set of suspicious deaths or a disease outbreak before it becomes clickbait and fuels hysteria will be critical. Ramping up medical intelligence efforts to include frontline methods and top expertise in molecular biology is thus of paramount importance.

Acknowledgments

The author is grateful to Commander Philip Bacchus of the Swedish Armed Forces National CBRN Defence Centre for his valuable comments and criticisms of the text.

References

1. Koblentz GP. *Living Weapons: Biological Warfare and International Security*. Ithaca, NY: Cornell University Press; 2011.
2. Lentzos F. *Biological Threats in the 21st Century: The Politics, People, Science and Historical Roots.* London: Imperial College Press; 2016.
3. Goodman MS, Lentzos F. Battles of influence: deliberate disinformation and global health security. Center for International Governance Innovation. Published August 24, 2020. Accessed September 1, 2021. https://www.cigionline.org/articles/battles-influence-deliberate-disinformation-and-global-health-security/
4. International Crisis Group. COVID-19 and conflict: seven trends to watch. Published March 24, 2020. Accessed November 30, 2021. https://www.crisisgroup.org/global/sb4-covid-19-and-conflict-seven-trends-watch
5. Nicomedes CJC, Avila RMA. An analysis on the panic during COVID-19 pandemic through an online form. *J Affect Disord.* 2020;276:14-22.
6. Chigada J, Madzinga R. Cyberattacks and threats during COVID-19: a systematic literature review. *S Afr J Inf Manag.* 2021;23(1):a1277
7. Williams CM, Chaturvedi R, Chakravarthy K. Cybersecurity risks in a pandemic. *J Med Internet Res.* 2020;22(9):e23692.
8. Chandra B, Gonzalez A. Managing chaos: biosecurity in a post-COVID-19 America. The Strategy Bridge. Published August 3, 2020. Accessed November 4, 2021. https://thestrategybridge.org/the-bridge/2020/8/3/managing-chaos-biosecurity-in-a-post-covid-19-america
9. DiEuliis D, Ellington AD, Gronvall GK, Imperiale MJ. Does biotechnology pose new catastrophic risks? *Curr Top Microbiol Immunol.* 2019;424:107-119.
10. Raina MacIntyre C, Engells TE, Scotch M, et al. Converging and emerging threats to health security. *Environ Syst Decis.* 2018;38(2):198-207.
11. Domaradskij IV, Orent LW. Achievements of the soviet biological weapons programme and implications for the future. *Rev Sci Tech.* 2006;25(1):153-161.
12. Palmer MJ. Learning to deal with dual use. *Science.* 2020; 367(6482):1057.
13. Powell K. How biologists are creating life-like cells from scratch. *Nature.* 2018;563(7730):172-175.
14. Carter SR, Warner CM. Trends in synthetic biology applications, tools, industry, and oversight and their security implications. *Health Secur.* 2018;16(5):320-333.
15. Pezoulas VC, Hazapis O, Lagopati N, et al. Machine learning approaches on high throughput NGS data to unveil mechanisms of function in biology and disease. *Cancer Genomics Proteomics.* 2021;18(5):605-626.
16. Lentzos F. How to protect the world from ultra-targeted biological weapons. *Bull At Sci.* 2020;76(6):302-308.
17. Nilsson EM, Sullivan OM, Anderson ML, et al. Reverse genetic engineering of simian rotaviruses with temperature-sensitive lesions in VP1, VP2, and VP6. *Virus Res.* 2021;302: 198488.
18. Holmes EC, Goldstein SA, Rasmussen AL, et al. The origins of SARS-CoV-2: a critical review. *Cell.* 2021;184(19):4848-4856.
19. Wallace R. *Carl von Clausewitz, the Fog-of-War, and the AI Revolution: The Real World Is Not a Game of Go.* 1st ed.

Cham, Switzerland: Springer International Publishing; 2018.
20. Budowle B, Murch R, Chakraborty R. Microbial forensics: the next forensic challenge. *Int J Legal Med.* 2005;119(6): 317-330.
21. Azoulay A. UNESCO embraces open science to shape society's future. *Nature.* 2021;593(7859):341.
22. European Commission. The EU's open science policy. Accessed September 19, 2021. https://ec.europa.eu/info/research-and-innovation/strategy/strategy-2020-2024/our-digital-future/open-science_en
23. Mitchell MJ, Billingsley MM, Haley RM, Wechsler ME, Peppas NA, Langer R. Engineering precision nanoparticles for drug delivery. *Nat Rev Drug Discov.* 2021;20(2): 101-124.
24. Petrenko VA. Autonomous self-navigating drug-delivery vehicles: from science fiction to reality. *Ther Deliv.* 2017; 8(12):1063-1075.
25. Singh JA. Project Coast: eugenics in apartheid South Africa. *Endeavour.* 2008;32(1):5-9.
26. Trump BD, Galaitsi SE, Appleton E, et al. Building biosecurity for synthetic biology. *Mol Syst Biol.* 2020;16(7): e9723.
27. Lentzos F, Goodman MS, Wilson JM. Health security intelligence: engaging across disciplines and sectors. *Intell Natl Secur.* 2020;35(4):465-476.
28. Lewis G, Jordan JL, Relman DA, et al. The biosecurity benefits of genetic engineering attribution. *Nat Commun.* 2020;11(1):6294.
29. Ledford H. Autopsy slowdown hinders quest to determine how coronavirus kills. *Nature*. May 7, 2020. doi:10.1038/d41586-020-01355-z
30. European Commission. *Commission Decision of 16.9.202: Establishing the Health Emergency Preparedness and Response Authority.* Brussels: European Commission; 2021. Accessed December 17, 2021. https://ec.europa.eu/health/sites/default/files/preparedness_response/docs/hera_2021_decision_en.pdf

Address correspondence to:
David Gisselsson, MD, PhD
Division of Clinical Genetics
Biomedical Center (BMC) C13
SE 221 84 Lund
Sweden

Email: david.gisselsson_nord@med.lu.se