July 2025

INSS
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

STRATEGIC FORUM
National Defense University

About the Authors

James Giordano is Director of the Center for Disruptive Technology and Future Warfare, Institute for National Strategic Studies (INSS), at the National Defense Univeristy. Diane DiEuliis is the Assistant Director and Distinguished Research Fellow in the Center for the Study of Weapons of Mass Destruction, INSS.

Key Points

- Modern commercial and custom-engineered drones provide low-cost solutions for both proximate and relatively long-distance precision strikes.
- The convergence of drone technologies with biosciences (such as gene editing, synthetic biology, and nano-biotechnology) and artificial intelligence introduces an escalating dual-use threat to national and international security.
- Drone-delivered bioweapons challenge existing detection, deterrence, and response protocols. Potential attack scenarios include targeted biological strikes via drone dispersal and drone-assisted assassination or sabotage.
- A proactive approach grounded in technology foresight, scenario planning, and international cooperation will be key to managing this complex threat environment.

Drone Delivery of Bioweapons: Responsibilities for Force Readiness

By James Giordano and Diane DiEuliis

The U.S. National Drone Association recently sponsored the inaugural international U.S. Military Drone Crucible Championship to provide a venue for American and allied military drone training, advanced piloting, operational utility, and countermeasure capability.[1] The relevance—and importance—of such incentives and initiatives is clear in light of iterative development, availability, and utilization of drone technology in military operations and potential manifestations of envisioned large-scale drone employment in kinetic and nonkinetic engagements.[2] Such developments become ever more relevant and critical, as iterative advancements in the biosciences (for example, synthetic biology, gene editing, nanoscale biomaterials) have potential to be used as novel weapons that could employ drone technology for more facile, effective, and efficient delivery to particular types of targets.[3]

Advances in such emerging technology change the character of conflict and can be used to incur disruptive effects—with potentially destructive manifestations—on day-to-day U.S. supply chains, logistics, mid- to long-term economic stability, and the balance of global power. Although these platforms have limitations regarding range, payload capacity, and survivability, they serve as a force multiplier by enabling persistent surveillance, precision strikes, and rapid response capabilities at relatively low cost. Such experience could certainly be used to further develop drone capability to capitalize on novel employment strategies aimed at pure disruption and to complicate doctrinal countermeasures to unmanned systems. Indeed, drones, ranging from commercially available systems to custom-engineered platforms, could be effectively and efficiently committed in a variety of battlespace scenarios. Their small size, affordability, and versatility make them attractive tools for adversaries seeking to leverage asymmetrical advantage.

Key attributes of drones include:

- Ease of modification: Commercial drones can be developed and/or modified to deliver a variety of types and volumes of payloads.
- Stealth and precision: Drones can evade radar and air-defense systems, enabling covert operations in urban or rural environments.
- Range and scalability: Advanced drones can operate over long distances and be deployed either individually (for granular, precision-engagements) or in swarms, fortifying their operational impact and value.

The accessibility of drones provides cost-efficient means of payload delivery in state-on-state engagements and lowers the barrier to entry for nonstate actors, including terrorist organizations and criminal networks, thereby creating a dispersed and decentralized threat that is challenging to monitor and mitigate.

The Threat of Dually-Usable Convergent Science and Technology

The dual-usability of convergent advanced drone technology and novel biotechnological tools (such as synthetic biology and gene editing) poses a further—and escalating—risk to global security.[4] As the concomitant sophistication and accessibility of these technologies increase, so does their potential misuse by state and nonstate actors for malicious purposes.

Synthetic biology and gene-editing technologies, such as CRISPR-Cas systems, represent transformative tools with vast potential in precision medicine, agriculture, and industrial processes. However, these same technologies have dual-use potential and can be repurposed to develop biological agents capable of targeting select individuals, particular populations, ecosystems, and/or specific critical resources.[5] Key capabilities of these bioscientific and technological tools include:

- Pathogen enhancement: Modifying existing pathogens to increase virulence, transmissibility, escape diagnostics, or to confer resistance to medical countermeasures.
- Precision bioengineering: Designing pathogens to target specific genetic and/or phenotypic markers within populations, enabling selective effects.
- Performance degradation: Engineering microorganisms, proteins, or other biological entities to degrade human performance.
- Environmental disruption: Engineering microorganisms to degrade infrastructure materials or disrupt ecosystems, creating widespread collateral damage; disruption of food, supply, and revenue chains; and destructive effect(s) within local, regional, and national economies.

Drone Delivery of Bioweapons: Capabilities, Counters—and Contingencies

When combined with the deployment capabilities of drones, these biotechnological innovations pose an unprecedented challenge to traditional security frameworks. Such synergy amplifies the threat of such weapons. Possible scenarios that illustrate the operational potential of this nexus include the following:

- Targeted attacks: Drones equipped with aerosol dispersal mechanisms can release bioengineered agents in specific locations, targeting critical infrastructure or densely populated areas. The (bioagent) payload could be engineered to spread contamination over a given target area, threatening enemy troop emplacements, undermining troop movements, and compromising adversary infrastructures and/or logistical hubs.
- Bioterrorism: State and nonstate actors could exploit drones to execute high-profile attacks, creating psychological, economic, and political disruptions. Since a planned bioterror attack in 1998, and again in the aftermath of 9/11, the use of crop dusters as delivery vehicles for biological or chemical weapons of mass destruction was of serious concern.[6] The advent of sophisticated drone technologies makes this concern much more viable.
- Diversion of commercial drones for malicious purposes: Drones that enable precision agriculture, frequently sourced from adversary nations such as China,

can be compromised or diverted to disrupt food/agricultural security.

- Assassination and sabotage: Precision bioengineering can enable the creation of agents designed to target specific individuals or groups based on genetic profiles, delivered by drones to high-profile targets in precise locations.

To be sure, this convergence creates tactical challenges for military—and civilian—forces tasked with deterrence, defense, and response. For example, drones were used by Chinese gangs to spread African swine fever in local farmers' pig populations to prompt pathogenic spread and induce high mortality rates among the herds, disrupting the balance of the local agricultural economy, creating regional food shortages, and destabilizing international pork markets. This effort was followed by a misinformation campaign about the spread of the disease, which then enabled gangs to introduce "favored farmers'" pigs into the markets. These pigs could in turn be sold at higher prices and return profits to the gangs and fortify their influence.[7] This example illustrates how drone delivery of bioagents could be utilized to deliver pathogens capable of affecting not just livestock but humans as well.

The increasing sophistication of drone-based biological weapons necessitates a reevaluation of existing military doctrines and operational paradigms. We argue that critical implications emerge in the following principal domains.

Detection and Prevention.

- Drone detection: Developing advanced radar, acoustic, and visual systems capable of identifying drones, particularly those designed for stealth operations.
- Surveillance: Enhancing capabilities to monitor environmental and public health indicators for early detection of bioweapon deployment.

Deterrence. The Department of Defense (DOD) has already begun to think about how to deter drone use by adversaries. The categories noted here, namely detection, countermeasures, and training/preparedness, can serve as denying benefits to adversaries that might have interest in utilizing drones for delivery of weapons of mass destruction or disruption (WMD-2). Aligned with this, DOD has developed an initial strategy and stood up a Joint Counter–Small Unmanned Aircraft Systems Office. These efforts will build the infrastructure and more institutionalized thinking about drones in the context of WMD-2. An existing problem is the generally low cost of drone creation for potential WMD-2 use versus the high cost that will be needed to defeat these systems specifically based on their intended use. Leveling this imbalance in cost will be necessary. Strategies that assist with this have been described in a recent Joint Staff publication, which highlights five "Ds" of deterrence: detection, definition, determination, disruption, and diminution.[8] As applied to drone threats, *detection* of threats from specific adversaries and *defining* the nature of those threats will enable more specific *determination* of how they can be best deterred. Drones could also be used to *disrupt* adversaries' bioweapon research, production, storage and deployment sites and capabilities, and in this way, could *diminish* resources required for current and future threats. Taken together, consideration of this five-D approach could enable a more prudent investment strategy for balancing the costs and benefits of drone deterrence.

Countermeasure Development. Defensive measures must include counter-drone systems that utilize technologies such as jamming, directed energy weapons, and drone swarms to neutralize hostile drones. Counter systems must be adaptable, delivered rapidly, and at scale—which may include directive defense industrial base changes and/or working more closely with allies and partners to do so. Additionally, bioagent defense research is crucial to enable early warning and enhanced biodetection, particularly in the environment, and accelerating the development of vaccines, therapeutics, and diagnostic tools to counter novel biological agents would be necessary. Also required would be investments in advanced counter-drone systems and electromagnetic warfare capabilities to intercept or neutralize drone deployments before they can achieve their intended disruptive effect. As simply shooting down a drone carrying such payloads

could still release biological material, advanced detection and early interception requirements are increased, disfavoring traditional elimination of threats in their terminal phase. Instead, earlier detection and downing over more favorable terrain would be required for defenders.

Preparedness. Military personnel must be prepared to operate in environments where biotechnological weapons may be used. This includes more comprehensive investigation of the impacts of biologically contested environments on specific operations and how they will vary across both areas of responsibility and mission capabilities. For example, a contaminated field and a contaminated airstrip have differing vulnerabilities in terms of how readily operations can be maintained. As well, the nature of contestation could vary between various operational environmental and seasonal conditions (for example, U.S. Southern Command and U.S. Africa Command).

Augmented Training. The contingencies mentioned should be reflected in training to include exercises that involve scenarios involving drone-delivered biological weapons. This includes training in the use of threat-agnostic protections (warfighter tools and protective gear, medical countermeasures, prophylactics, and so forth) that can mitigate the effects of any drone-delivered biological weapons, regardless of specificity. While not inclusive of every aspect of threat, such training can allow for systematized awareness in the deployed force to more readily, accurately, and effectively recognize and respond to the growing drone threat.

Interagency Coordination. Strengthening collaboration among military, intelligence, public health, and law enforcement agencies to create a unified assessment and response framework would be required. Elsewhere, we have proposed a four-thrust approach toward technological threat identification, mitigation, and prevention. This approach entails 1) increasing (both professional and public) awareness of risks and threats posed by emerging technology; 2) quantifying the actual level and extent of burden and harm posed by particular risks and threats so as to prioritize resources necessary to address and engage these risk factors; 3) engaging multiple resources and services to mitigate harms posed by prioritized threats; and 4) deploying resources to prevent peer-competitor and adversarial development and use of technologies that cold pose continuing and/or future threat.[9] However, as we have noted, while intragovernmental collaboration and cooperation is necessary to these actions, the most effective and efficient effort would entail a whole-of-nation effort to coordinate key elements of government (bipartisan political conjoining in policy support; the military and intelligence communities), the private sector (research institutions), and industry to establish requisite scalability and flexibility in preparedness and response.[10]

Intelligence and Risk Assessment. Enhanced intelligence capabilities are essential for identifying peer-competitor and potential adversaries' use of drones and developing and implementing technological advancements necessary to identify, track, and deter such threats. This includes:

- Threat profiling: Monitoring state and nonstate actors known to have access to both drone and dually-usable biotechnologies. Enhancing real-time monitoring of drone procurement and integration into operational theaters, with particular attention to end-users and modifications that might suggest a bioweapon payload profile.
- Supply chain monitoring: Identifying and disrupting the flow of materials and knowledge required to develop bioweapons. With the expansion of DNA synthesis and other synthetic biology companies (enterprises) around the globe, access to genetic tools and kits has expanded beyond adversary states. The United States has made headway in developing screening guidance for synthetic DNA providers and expanded to include desk-top synthesizers. These are just two categories of biological materials and equipment that would be utilized in the development of biological threat agents.[11]

Ethical and Legal Considerations

The use of drones to deliver such novel technological weapons raises several ethical and legal challenges both within the military and more broadly. While certainly not a new concern, such considerations should be reframed

for clarified focus on the use of drone-based nonconventional weapons to include:

- Attribution: Identifying the perpetrators of drone-based bioweapon attacks can be difficult, particularly if and when the drone is destroyed in executing the mission and/or nonstate actors or proxy forces are involved.
- Accountability: Ensuring that states adhere to international norms, such as the Biological Toxins and Weapons Convention. Regulations for drone deployment can be irrelevant if drones are clandestinely or covertly used (see above) and if state or nonstate actors exploit legal loopholes.
- Proportionality: Developing response protocols that balance the need for decisive action with the potential for escalation and collateral damage (could/should a drone-based engagement be countered with a non-drone conventional weapon and/or human actor response?).

The decision to deploy any novel bioagent carries considerable risks. The inherent ambiguity, given the uniqueness of such agents, could trigger a miscalculation, leading to unanticipated and/or runaway effects that pose risk for more widespread (for example, pandemic) manifestations. The risks associated with such effects—militarily, economically, politically, and medically—would be weighed heavily against any perceived tactical advantage.

As drones and bioagent technologies are iteratively developed and advanced, it will be crucial for the United States and its allies to monitor, navigate, and address these complexities while upholding established principles of discrimination and necessity of attribution and proportionality in response.

Responding to the Threat

The integration of artificial intelligence (AI) into drone and biotechnological device platforms represents a further development in this threat evolution. AI-driven systems coupled with open-source drone (and bio) technology lowers the barriers for adversaries to develop and deploy these technologies as weapons.[12] The use of AI could enable increasingly autonomous decisionmaking, swarm coordination, and precision targeting of drones, which when taken either separately or in combination further could complicate defensive efforts.[13] To address this evolving threat, we propose a proactive and forward-looking multifocal approach:

- Technology foresight: Anticipate capabilities of emerging technologies and their potential misuse. Elsewhere, we have described our conception of what projects and programs of technology foresight should entail and obtain.[14] Considering the pace and extent of scientific and technological research and its translation to operational applications, we have noted that foresight and analyses are most capable within a 5- to 10-year future period, based on assessment of scientific and technological programs, projects, and deliverables in extant research and development pipelines; the readiness levels of these products; and the viable vectors for use in various types of military missions. While forecasting beyond 10 to 15 years has proved somewhat more difficult and problematic, current and near-term iterations and capabilities of machine learning and AI, when coupled with expanded efforts in multidomain (that is, research, commercial, economic, military, political) surveillance and evaluation, may overcome existing constraints of forecast analytics, preparedness, and planning.[15]
- Scenario planning: Move toward developing and assessing response protocols for a range of plausible threat scenarios.
- International Collaboration: Engage allies, international organizations, and the private sector to share knowledge, develop standards, and build collective resilience and coordinated response protocols and parameters.

Summary

The convergence of drone technology and emerging biosciences represents a formidable challenge to global security. As history often demonstrates, the misuse of innovative technologies often outpaces an ability to expediently respond. We posit that vigilance, foresight, and preparedness will be vital to address these challenges and protect against the exploitation of emerging technology for malicious purposes. For military forces, this emerging threat necessitates a paradigm shift in the detection,

mitigation, and prevention of drone-based attacks. Indeed, the military's role in this endeavor is critical—not only as a defensive force but also as a leader in shaping the ethical and legal frameworks that govern the use of emerging technologies. Thus, it is important to invest in fostering interagency and international collaboration, advanced surveillance systems, and developing robust countermeasures to mitigate the risks associated with these technologies while preserving strategic and operational stability.

Notes

[1] "USNDA Forms Inter-Service U.S. Military Competitive Drone Teams, U.S. Marines First to Fight in International Military Drone Crucible Championship on Independence Day Week," *PR Newswire*, January 21, 2025, https://www.prnewswire.com/news-releases/usnda-forms-inter-service-us-military-competitive-drone-teams-us-marines-first-to-fight-in-international-military-drone-crucible-championship-on-independence-day-week-302356661.html.

[2] James Giordano, "Opening the Replicator Program's Pandora's Box," *National Defense*, December 27, 2023, https://www.nationaldefensemagazine.org/articles/2023/12/27/opening-the-replicator-programs-pandoras-box.

[3] *2022 National Defense Strategy of the United States of America, Including the 2022 Nuclear Posture Review and the 2022 Missile Defense Review* (Washington, DC: Department of Defense, 2022).

[4] Joseph DeFranco and James Giordano, "Dark Side of Delivery: The Growing Threat of Bioweapon Dissemination by Drones," *DefenceIQ*, January 24, 2020, https://www.defenceiq.com/cyber-defence-and-security/articles/the-dark-side-of-delivery-the-growing-threat-of-bioweapon-dissemination-by-drones.

[5] Diane DiEuliis and James Giordano, "Balancing Act: Precision Medicine and National Security," *Military Medicine* 187, Supplement 1 (January–February 2022), 32–5, https://doi.org/10.1093/milmed/usab017.

[6] Michelle Caruso et al., "Toxic Terror: Larry Wayne Harris and William Leavitt Are Arrested for Plotting a Biological Attack on New York City Subways in 1998," *New York Daily News*, February 20, 1998, updated January 12, 2019, https://www.nydailynews.com/2016/02/17/toxic-terror-larry-wayne-harris-and-william-leavitt-are-arrested-for-plotting-a-biological-attack-on-new-york-city-subways-in-1998/; "FBI Still Fears Threat From Crop-Dusters," NBC News, April 22, 2004, https://www.nbcnews.com/id/wbna4808551.

[7] Liu Zhen, "Chinese Criminal Gangs Spreading African Swine Fever to Force Farmers to Sell Pigs Cheaply So They Can Profit," *South China Morning Post* (Hong Kong), updated December 17, 2019, https://www.scmp.com/news/china/politics/article/3042122/chinese-criminal-gangs-spreading-african-swine-fever-force.

[8] James Giordano, *Deterrence and the Integration of Chemical, Biological, and Data and Cybersciences and Technologies: Disruptive Possibilities and Defensive Potential*, Strategic Multilayer Assessment Group–Joint Staff/J-3 (Washington, DC: The Joint Staff, April 2024).

[9] Joseph Defranco et al., "Emerging Technologies for Disruptive Effects in Non-Kinetic Engagements," *HDIAC Journal* 6, no. 2 (Summer 2019), 49–54, https://hdiac.dtic.mil/articles/emerging-technologies-for-disruptive-effects-in-non-kinetic-engagements/.

[10] Joseph DeFranco et al., "Emerging Bio-Technologies for Disruptive Effects in Grey Zone Engagements," in *Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies*, ed. Mitt Regan and Aurel Sarel (New York: Oxford University Press, 2024), 237–49.

[11] *Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA* (Washington, DC: Department of Health and Human Services, October 2010), https://aspr.hhs.gov/legal/syndna/Documents/syndna-guidance.pdf.

[12] James Giordano, "Chem-Bio, Data, and Cyberscience and Technology in Deterrence Operations," *HDIAC Journal* 8, no. 1 (2024), 26–35, https://hdiac.dtic.mil/wp-content/uploads/2024/06/HDIAC_2024_Vol_8_No_1_web_final.pdf.

[13] Daniel Howlader and James Giordano, "Advanced Robotics: Changing the Nature of War and Thresholds and Tolerance for Conflict—Implications for Research and Policy," *Journal of Philosophy, Science & Law* 13, no. 2 (May 2013), 1–19, https://www.pdcnet.org/collection/fshow?id=jpsl_2013_0013_0002_0001_0019&pdfname=jpsl_2013_0013_0002_0002_0020.pdf&file_type=pdf.

[14] Diane DiEuliis and James Giordano, "Addressing the Threats of Emerging Biotechnologies," *National Defense*, September 14, 2022, https://www.nationaldefensemagazine.org/articles/2022/9/14/commentary-addressing-the-threats-of-emerging-biotechnologies; Joseph DeFranco and James Giordano, "Mapping the Past, Present, and Future of Brain Research to Navigate the Directions, Dangers, and Discourses of Dual-Use, *EC Neurology* 12, no. 1 (2020), 1–6, https://ecronicon.net/assets/ecne/pdf/mapping-the-past-present-and-future-of-brain-research-to-navigate-directions-dangers-and-discourses-of-dual-use.pdf.

[15] Diane DiEuliis and James Giordano, "Regarding and Reducing Risks of the Biotechnology Revolution, *CBNW*, June 24, 2022, https://nct-cbnw.com/regarding-and-reducing-risks-of-the-biotechnology-revolution-2/; Prashant Desai et al., "Addressing and Managing Systemic Benefit, Burden, and Risk of Emerging Neurotechnology," *AJOB Neuroscience* 13, no. 1 (2022), 68–70; Joseph DeFranco et al., "The Emerging Neurobioeconomy: Implications for National Security," *Health Security* 18, no. 4 (July–August 2020, 267–77, https://doi.org/10.1089/hs.2020.0009; Giordano, "Chem-Bio, Data, and Cyberscience and Technology in Deterrence Operations."

INSTITUTE FOR NATIONAL STRATEGIC STUDIES

The Center for Disruptive Technology and Future Warfare produces cutting-edge analyses and research on artificial intelligence/cyber systems; autonomous and semi-autonomous weapons systems; novel and emerging biological, chemical, and electromagnetic weapons; quantum systems, and nanoengineered materials and devices; and assesses the implications of these technologies for national security policy and strategy.

INSS
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

NDU Press

The Strategic Forum series presents original research by members of NDU as well as other scholars and specialists in national security affairs from the United States and abroad. The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Defense Department or any other agency of the Federal Government.

James Giordano
Director
CDTFW

Denise Natali
Director
INSS

William T. Eliason
Director
NDU Press