The US Army War College Quarterly: Parameters

Volume 52
Number 2 *Volume 52, Number 2 Summer Issue*

Article 13

Summer 5-18-2022

# InfoSwarms: Drone Swarms and Information Warfare

Zachary Kallenborn

## Recommended Citation

Zachary Kallenborn, "InfoSwarms: Drone Swarms and Information Warfare," *Parameters* 52, no. 2 (2022): 87-102, doi:10.55540/0031-1723.3154.

# InfoSwarms: Drone Swarms and Information Warfare

Zachary Kallenborn

ABSTRACT: Drone swarms, which can be used at sea, on land, in the air, and even in space, are fundamentally information-dependent weapons. No study to date has examined drone swarms in the context of information warfare writ large. This article explores the dependence of these swarms on information and the resultant connections with areas of information warfare—electronic, cyber, space, and psychological—drawing on open-source research and qualitative reasoning. Overall, the article offers insights into how this important emerging technology fits into the broader defense ecosystem and outlines practical approaches to strengthening related information warfare capabilities.

**Keywords: information warfare, drone swarms, unmanned systems, cyberwarfare, electronic warfare**

Drone swarms are here.[1] In Israel's 2021 conflict with Gaza, the country's military became the first to deploy a drone swarm in combat. During the ongoing conflict between Russia and Ukraine, Russia deployed the Kalashnikov KUB-BLA loitering munition, which reportedly is (or will be) capable of swarming.[2] Russia also possesses a yet-to-be-deployed Lancet-3 munition with the potential capability to create aerial minefields to target drones and other aircraft.

The United States and its allies and adversaries are pursuing collaborative drone-swarm technology. This pursuit is no surprise. Drone swarms have applications for every military service across every area of conflict, from infantry support and logistics to nuclear deterrence.[3] Military leaders across the Joint force must consider how drone swarms relate to existing capabilities and forms of warfare as the technology matures and enters the battlefield. These ideas should inform future concepts, acquisition decisions, exercises, training, plans, and operations to account for friendly and adversarial use. This article examines one aspect of a larger challenge: drone swarms and information warfare.

[1] Sebastien Roblin, "Russian Drone Swarm Technology Promises Aerial Minefield Capabilities," *National Interest* (website), December 30, 2021, https://nationalinterest.org/blog/reboot/russian-drone-swarm-technology-promises-aerial-minefield-capabilities-198640.

[2] "ZALA Aero Company Successfully Tests KUB-BLA Kamikaze Drone," Air Recognition (website), November 12, 2021, https://www.airrecognition.com/index.php/news/defense-aviation-news/2021/november/7857-zala-aero-company-successfully-tests-kub-bla-kamikaze-drone.html; and Will Knight, "Russia's Killer Drone in Ukraine Raises Fears about AI in Warfare," *Wired* (website), March 17, 2022, https://www.wired.com/story/ai-drones-russia-ukraine/.

[3] Zachary Kallenborn and Philipp C. Bleek, "Swarming Destruction: Drone Swarms and Chemical, Biological, Radiological, and Nuclear Weapons," *Nonproliferation Review* 25, no. 5-6 (2019): 523–43.

Although drone swarms may operate on land, at sea, in the air, and even in space, they are fundamentally information-dependent weapons. The common denominator of every swarm is the need to maintain stable communication links between drones and ensure information is processed efficiently and appropriately. Indeed, swarms are "multiple unmanned systems capable of coordinating their actions to accomplish shared objectives."[4] Many of the unique strengths of swarming also derive from information sharing.

The advantages of drone swarms stem from three key areas: swarm size, customization, and diversity.[5] Each area depends on effective information management. Larger swarms with more sensors and munitions are more capable and can enable mass attacks; however, the swarm must handle inputs from more drones. Flexible swarms add or remove drones to meet commander needs, may break into smaller groups to attack from multiple directions or strike different targets, and handle changes to information inputs as drones are added or removed. Diverse swarms can incorporate different types of munitions and sensors and allow closely integrated, multidomain strikes, add new types of information sources, and create coordination challenges when the drones move at different speeds with different environmental risks. Information failure means risk of collision and loss of capability.

These capabilities enable novel tactics supported by information sharing. As Paul Scharre writes, "Swarming will be a more effective, dynamic, and responsive organizational paradigm for combat."[6] Swarms can concentrate fire on targets or disperse and reform to counterattack. Achieving these feats requires high levels of stable communication.[7]

Support technologies depend on information as well. Machine vision—the ability of machines to see—requires a high volume of data to train the algorithms. Sensor drones use these algorithms to collect and share information on adversarial defenses, possible targets, and environmental hazards.[8] Like individual drones, the swarm as a whole or the external control systems must process the high volume of information collected in the field. Processing speeds affect the swarm's battlefield value because slower algorithm speeds mean slower decision making.[9] Although

[4] Kallenborn and Bleek, "Swarming Destruction."

[5] Zachary Kallenborn, "The Era of the Drone Swarm Is Coming, and We Need to Be Ready for It," Modern War Institute at West Point (website), October 25, 2018, https://mwi.usma.edu/era-drone-swarm-coming-need-ready/.

[6] Paul Scharre, "How Swarming Will Change Warfare," *Bulletin of the Atomic Scientists* (website), October 22, 2018, https://thebulletin.org/2018/11/how-swarming-will-change-warfare/.

[7] Scharre, "Swarming Will Change Warfare."

[8] Zachary Kallenborn, "Swarm Talk: Understanding Drone Typology," Modern War Institute at West Point (website), December 10, 2021, https://mwi.usma.edu/swarm-talk-understanding-drone-typology/.

[9] Paul Scharre, "Counter-Swarm: A Guide to Defeating Robotic Swarms," War on the Rocks (website), March 31, 2015, https://warontherocks.com/2015/03/counter-swarm-a-guide-to-defeating-robotic-swarms/.

a swarm may not incorporate machine vision, human controllers will face similar challenges as the swarm scales in size.

Information dependence means drone swarms must be considered in the context of information warfare. According to the Congressional Research Service, the US government does not have an official definition for information warfare. Practitioners typically define information warfare as "strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations."[10] This strategy includes electronic warfare, elements of cyberwarfare, and psychological warfare. Space warfare is included here because position, navigation, timing information, and satellite-based communication are critical information sources for unmanned systems.[11]

Of course, noting the information dependence does not mean actors will successfully recognize or exploit this dependency. Although the Russian military has long recognized the importance of electronic warfare in countering drones, the military appears to have struggled in implementing this knowledge during the Ukraine conflict. For example, video released on social media seems to show Ukrainian drones in close proximity to Russian vehicles with no Russian electronic-warfare protection.[12] The Russian military and others may also struggle to implement this knowledge in the cyber, space, and psychological warfare domains.

This article examines the relationship of drone swarms to the four dimensions of information warfare (electronic, cyber, space, and psychological) and explores artificial intelligence (AI) and robotics, which support the other areas and affect drone-swarm information-warfare vulnerabilities. Policy recommendations conclude the article.

## Electronic Warfare

In the Center for the Study of the Drone at Bard College's review of counterdrone systems, electronic jamming was the most popular counterdrone interdiction system.[13] This popularity is no surprise; electronic jamming represents a potentially cheap, reusable approach to defeating drones, swarming or not. Humans must provide drones with mission parameters, firing decisions, and, sometimes, physical control. Interrupting control and information sharing within

[10] Catherine A. Theohary, *Defense Primer: Information Operations*, IF10771 (Washington, DC: Congressional Research Service, December 2020).

[11] Theohary, *Defense Primer*.

[12] Samuel Bendett (@SamBendett), "If these are indeed Ukrainian drones in such a close proximity to Russian vehicles, where is the Russian counter-UAV and EW protection?," Twitter, March 19, 2022, 8:54 AM, https://twitter.com/SamBendett/status/1505165776814288897.

[13] Arthur Holland Michel, *Counter-Drone Systems* (Annandale-on-Hudson, NY: Center for the Study of the Drone, February 2018).

the swarm disrupts the drones.  If communication is disrupted, humans cannot set or revise the mission or direct strikes or issue retreat orders. Drone swarms depend even more on communication—particularly, communication on the electromagnetic spectrum.

Although drones can create swarms according to simple rules, communication is essential for complex behaviors, particularly  for swarming in a military context in which battlefields have varied terrain, combatant numbers and configurations shift, and a range of combat tactics are employed.[14] Thus, communication is necessary to prevent drone-swarm collision and coordinate movements and attack decisions. If the drones cannot communicate, the swarm cannot function as a coherent unit, coordinate searches for targets, or share successful identifications. In addition, the drones cannot coordinate strikes in which some drones attack one target and others another. The value of a drone swarm is lost without communication.

Electronic attacks can mimic friendly signals and manipulate the communication of the whole swarm. For instance, Iran reportedly captured a Lockheed Martin RQ-170 Sentinel drone by jamming the drone's communication and manipulating the Global Positioning System to force it to land in Iran in 2011.[15] False signals could steer an aerial swarm into a mountain, building, or other obstacle. If a state allows drones to fire without human control (which is by no means certain), adversaries could also send a signal indicating an adversary is at a friendly position, potentially causing the swarm to fire on the position.

The communication architecture—and, therefore, the methods of disrupting or manipulating the drone swarm—vary among different swarms.[16] Swarm communication typically relies on the electromagnetic spectrum—radio waves (for example, Wi-Fi), infrared, and optical—but acoustic signals are likely necessary for underwater drones because electromagnetic signals do not propagate well underwater.[17] Thus, spectrum management is important to ensure signals within and among the swarm and any control station are deconflicted. The swarm control architecture requires signal delivery to the correct drone, which presents a challenge if drones in the swarm are disabled or destroyed.

[14] Maaike Verbruggen, *The Question of Swarms Control: Challenges to Ensuring Human Control over Military Systems*, Non-Proliferation and Disarmament Paper no. 65 (Brussels: EU Non-Proliferation and Disarmament Consortium, 2019).

[15] Scott Peterson, "Exclusive: Iran Hijacked US Drone, Says Iranian Engineer," *Christian Science Monitor* (website), December 15, 2011, https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer.

[16] Xi Chen, Jun Tang, and Songyang Lao, "Review of Unmanned Aerial Vehicle Swarm Communication Architectures and Routing Protocols," *Applied Sciences* 10, no. 10 (2020).

[17] John Heidemann, Milica Stojanovic, and Michele Zorzi, "Underwater Sensor Networks: Applications, Advances, and Challenges," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 370, no. 1,958 (2012): 158–75.

How information propagates throughout the swarm may vary, too, which may affect the mechanics of disrupting or maintaining communication.[18] In a swarm with centralized control, a single leader may coordinate tasks assigned to each member of the swarm. In swarms with decentralized control, drones communicate with the drones nearest them, leading to emergent flocking behaviors. In theory, this action removes the need for global communication. But the simple algorithms that enable decentralized control may be insufficient for complex, dynamic military contexts.

Future developments may reduce swarm electromagnetic spectrum dependence. New technologies offer communication channels according to different physical principles, such as quantum communication.[19] Alternatively, drones could coordinate their actions indirectly through stigmergy.[20] Insects such as ants leave pheromone traces on potential food sources. The ants that follow hone in on the traces and leave their pheromones if they, too, find food. Advanced drone swarms could adopt similar methods.

Ants offer another lesson for drone swarms: diversity in roles. Ants in a colony adopt specialized roles, most obviously between queen and worker ants. Likewise, swarms may incorporate communication drones that dedicate available onboard power to strengthening signals, serve as alternate nodes to exchange communication, or use a different signal type to issue retreat orders. Drone swarms could also blend centralized and decentralized communication approaches to increase resiliency. For example, the swarm may rely on decentralized communication and have a backup centralized communication system to combat jamming. This approach would require significant technical development to prevent conflict between the two communication approaches.

As drone swarms grow more autonomous, less information from electromagnetic spectrum-based sources originating outside the swarm is necessary, and less need for human input means less need for some communication channels. This autonomy, however, comes with a trade-off in new opportunities to manipulate or disrupt the autonomous systems.

In theory, an advanced drone swarm could become independent from external control, but policy and technical challenges place an upper bound on autonomy. Current Department of Defense policy does not allow semiautonomous weapons aboard unmanned platforms to select and engage targets if communications are

[18] Verbruggen, *Swarms Control*.

[19] Martin Giles, "Explainer: What Is Quantum Communication?," *MIT Technology Review* (website), February 14, 2019, www.technologyreview.com/s/612964/what-is-quantum-communications/.

[20] Ralph Beckers, Owen E. Holland, and Jean-Louis Deneubourg, "From Local Actions to Global Tasks: Stigmergy and Collective Robotics," in *Prerational Intelligence: Adaptive Behavior and Intelligent Systems without Symbols and Logic*, ed. Holk Cruise, Jeffrey Dean, and Helge Ritter (Dordrecht, NL: Springer Science, 2000), 2:1008–22.

degraded, nor can autonomous weapons target human beings with lethal force without meaningful human input.[21] Popular resistance will likely constrain change because people already fear robots gone wild. Autonomous, complex strategic decisions such as assessing the value of a target to an overall war effort are likely to be impossible without generalized AI, which is unlikely to emerge in the near term, if ever. So, some electronic communication will be needed for the foreseeable future. Electronic warfare is also increasingly tied to cyberwarfare.

## Cyberwarfare

Cyberattacks may seek to disable, control, manipulate, or exfiltrate information from drone swarms. Swarms necessarily possess all the cybersecurity vulnerabilities of individual drones, including vulnerability to deauthentication attacks (preventing the controller from operating the drone), code injection, and code alteration, exploitation of zero-day vulnerabilities, and exfiltration of data.[22] The incorporation of swarming introduces the interception, manipulation, and disruption of interswarm communication and the algorithms that manage collective swarm behavior, thereby broadening the attack surface. More drones also means more opportunities to attack the system.

Cyberattacks could drone control systems through deauthentication attacks or code injections or alterations. Disabling human control or code alterations that immobilize drone engines or propellers may cause the swarm to crash. Falling drones could collide with other drones or other friendly assets. Disabling sensors could cause the drone swarm to fly blindly, resulting in collisions or preventing the identification of adversary defenses and other targets of interest. As a civilian example, researchers in July 2015 exploited cyber vulnerabilities to disable the brakes on a Jeep Cherokee®.[23] Limiting drone movement provides adversaries with a battlefield advantage. More subtly, cyberattacks may exploit drone-swarm information processing algorithms. Simple manipulations of drone control and task allocation algorithms achieved through the provision of incorrect data, replay attacks (repeating or delaying valid information transfers), injections of nefarious code, or the alteration of existing code could cause significant disruptions. If a manipulation prevents drones from detecting one another, they may collide. A failure to detect an environmental hazard may cause a crash by simply feeding old video or image data so the swarm does not "see" the building in front of it. Because errors are inevitable, code alterations that increase the risk of

[21] Ashton B. Carter, *Autonomy in Weapons Systems*, Department of Defense Directive 3000.09 (Washington, DC: Office of the Secretary of Defense, November 2012).

[22] C. G. Leela Krishna and Robin R. Murphy, "A Review of Cybersecurity Vulnerabilities for Unmanned Aerial Vehicles," in *2017 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR)* (New York: Institute of Electrical and Electronics Engineers, 2017).

[23] Mahmoud Hashem Eiza and Qiang Ni, "Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cyber Security," *IEEE Vehicular Technology Magazine* 12, no. 2 (June 2017).

error (but that do not necessarily cause one) may go undetected for a long time. An adversary-induced error may appear as a normal computer error.[24] Alternatively, cyber manipulations may slow information processing, decision making, or object recognition and make the swarm more vulnerable to counterswarm defenses. Algorithm sabotage could even occur during the production process.

Advances in machine learning and related technologies allow adversaries to create and disseminate highly sophisticated fake images and videos or use cyber infiltration to inject them into data collections.[25] Fake data may lead image and video analysis software to incorrect conclusions, missed threats, or noncombatant targeting. If the same software is used in multiple unmanned systems, adversaries could cause massive harm.

Most significantly, adversaries could redirect the drone swarm to attack friendly targets through code alteration to the control algorithm or feeding incorrect data so the swarm believes a friendly target is an adversary.[26] Adversaries would turn the swarms' capabilities to their gain. Alternatively, adversaries could order the swarm to leave a threatened area or move into adversarial fire. Adversaries might also render the swarm safe for collection and study to gain unique intelligence on the swarm's capabilities. Vulnerability to cyber manipulation and levels of autonomy are interrelated.

More autonomy means more complex computing systems with more opportunities for exploitation and greater risk of error. Drones with autonomous navigation, movement, or targeting systems can operate without human control and can be manipulated. Likewise, coordination is likely to be more difficult with larger, heterogeneous swarms, which raises the risk of catastrophic failure. Identifying infiltration is also more challenging with larger swarms because adversaries may attack only one drone within the swarm.

Finally, adversaries could seek to exfiltrate data from the swarm by accessing communication links between the drones or between the drones and the control station or software and firmware in the internal control system of the drones themselves. These tactics could allow adversaries to collect intelligence on the location and activity of the swarm to improve defenses, retreat from an anticipated attack area, or prepare countermeasures as appropriate. Data exfiltration may

[24] *Duffel Blog* reporters 29 Reasons Why and Veishnoriets, "Point/Counterpoint: Future Wars Will Be Fought with AI Robots vs. 'Microsoft Word Is Not Responding,' " *Duffel Blog*, May 30, 2019, www.duffelblog.com/2019/05/point-counterpoint-future-wars-will-be-fought-with-ai-robots-vs-microsoft-word-is-not-responding/.

[25] Patrick Tucker, "The Newest AI-Enabled Weapon: 'Deep-Faking' Photos of the Earth," *Defense One* (website), March 31, 2019, www.defenseone.com/technology/2019/03/next-phase-ai-deep-faking-whole-world-and-china-ahead/155944/?oref=d-topstory.

[26] Scharre, "Counter-Swarm."

also enable more disruptive operations through a better understanding of the algorithms and programs that enable multiple drones to operate as swarms. This understanding would also better enable actors to create their own swarms.

## Space Warfare

Drone swarms typically rely on space assets for geolocation, and swarms that operate over the horizon require space assets for command and control. If satellites are disabled or destroyed, the swarms may not operate effectively—or at all. Recent technological developments, however, suggest the space domain may be less of a dependency over time and the most likely dimension of information warfare to stop being a drone-swarm requirement.

Many drone swarms rely on the Global Navigation Satellite System (GNSS) to guide them, and GNSS waypoints can be used to define the paths followed or the areas to avoid, identify targets of interest (such as the location of adversarial installations for intelligence collection), and y guide the swarm back to launch positions. Satellites may also serve as relays for command-and-control information.

Currently, drone swarms operate at relatively short ranges at which satellite communication is unnecessary. As the technology evolves, swarms may operate at longer ranges and these greater distances will likely require satellite-based communication for updating mission objectives, giving permissions, or providing other commands. In the future, communication among drones in a swarm may even require space assets to cover long distances.

Disabling or destroying satellites would prevent swarms reliant on satellites for geolocation or command orders from operating effectively. The drones would become ineffective and start wandering without knowing what to do or where to go. In a world where adversarial military force depends largely on unmanned systems, disabling geolocation over a wide area could prove devastating.

Advances in technology may reduce or possibly mitigate space-based risks. Swarms could use external GNSS nodes to aid in localization. One research team used Global Positioning System-linked buoys to allow underwater drones to locate their positions without direct access to the system.[27] The buoys released a periodic signal that underwater drones sensed to infer their location. A similar concept could aid ground or aerial vehicle geolocation by using signals transmitted from a known location (such as a support vehicle). Alternatively, new navigation concepts may remove the need for GNSS, though the degree

[27] Jules S. Jaffe et al., "A Swarm of Autonomous Miniature Underwater Robot Drifters for Exploring Submesoscale Ocean Dynamics," *Nature Communications* 8, no. 1 (January 2017).

to which these concepts will be successful in a military context is unclear.[28] As with electronic warfare, greater drone autonomy lowers the need for external, space-based signals.

## Psychological Warfare

Drone swarms have the least relevance for psychological warfare. The exception is for possibly spreading propaganda pamphlets, however, swarms appear to have few, if any, meaningful advantages over existing means of spreading propaganda. Nevertheless, drone swarms—and autonomous weapons more broadly—may be objects of misinformation, disinformation, and malinformation to the extent global and public norms form around the use of swarms and autonomous weapons. Growing movements are seeking to ban autonomous weapons due to concerns over risks to civilians and the ethics of abandoning human control. Increasingly large constituencies support the movement, including in some NATO member countries. For instance, 72 percent of Germans oppose the use of autonomous weapons, according to a January 2019 Ipsos poll.[29] Likewise, armed, fully autonomous swarms may pose psychological impacts and risks akin to traditional weapons of mass destruction due to the combination of mass casualty potential and the brittleness of current machine vision systems.[30] The term "weapons of mass destruction" carries strong normative implications with stigmas around their use and proliferation.[31]

Regardless of whether these public movements translate into changes in global policy, they may create opportunities for strategic information operations to sow division. For example, actors may amplify claims about the use of swarms and autonomous weapons to encourage opposition to a war effort, both internally and with partner nations. Conversely, actors may make false accusations against others to achieve the same effects. The challenges of verifying whether an autonomous weapon is truly autonomous make separating truth from fiction difficult.[32] The autonomy of a drone swarm may be easier to prove because a person could potentially control a small swarm consisting of dozens of drones, but no person could reasonably control a few thousand drones. Disproving false claims about autonomous drone-swarm use would be much harder.

[28] Evan Ackerman, "This Autonomous Quadrotor Swarm Doesn't Need GPS," *IEEE Spectrum* (website), December 27, 2017, https://spectrum.ieee.org/this-autonomous-quadrotor-swarm-doesnt-need-gps.

[29] Chris Deeney, "Six in Ten (61%) Respondents across 26 Countries Oppose the Use of Lethal Autonomous Weapon Systems," Ipsos (website), January 22, 2019, https://www.ipsos.com/en-us/news-polls/human-rights-watch-six-in-ten-oppose-autonomous-weapons.

[30] Zachary Kallenborn, *Are Drone Swarms Weapons of Mass Destruction?*, Future Warfare Series no. 60 (Maxwell Air Force Base, AL: US Air Force Center for Strategic Deterrence Studies, 2020)

[31] Patricia Shamai, "Name and Shame: Unraveling the Stigmatization of Weapons of Mass Destruction," *Contemporary Security Policy* 36, no. 1 (2015).

[32] Zachary Kallenborn, "If a Killer Robot Were Used, Would We Know?" *Bulletin of the Atomic Scientists* (website), June 4, 2021, https://thebulletin.org/2021/06/if-a-killer-robot-were-used-would-we-know/.

## Artificial Intelligence and Robotics

Advances in AI and robotics underpin all aspects of drone swarms and affect vulnerability and resilience to information warfare. Improvements in these technologies may lead to better targeting algorithms, swarm task allocation algorithms, and larger and more complex swarms and also affect electronic warfare, cyberwarfare, and space warfare systems that may be used by or against swarms. Greater use of AI and robotics on the battlefield may also create more opportunities for psychological warfare.

Robotics and AI could improve offensive electronic warfare and cyberwarfare capabilities. Machine learning could strengthen electronic warfare targeting and create more effective and automated cyberattacks. For instance, machine learning can enable better spectrum and power allocation, phishing detection, network intrusion detection, and other activities.[33] Indeed, China's People's Liberation Army Strategic Support Force is reportedly integrating machine learning with both cyberwarfare and electronic warfare.[34] Additionally, advances in machine learning could allow users to add better deep fakes to friendly or adversarial data sets via cyber means.[35] Researchers are also exploring the use of robots as platforms for electronic attacks and cyberattacks.[36]

Advancements in AI are also likely to improve electronic, cyber, and space countermeasures. Cyber defense techniques based on AI offer significant benefits to cyber intrusion detection, including improved accuracy, automated response, and throughput.[37] Alternatively, robotic systems could be used to form an ad hoc communications network where other systems are degraded or destroyed. For example, Swarm Technologies' SpaceBEE satellites form communication networks for Internet-connected devices.[38] Individual or multiple robots could serve as intermediaries to support stable communication.

[33] Vitaly Ford and Ambareen Siraj, "Applications of Machine Learning in Cyber Security" (working paper, 27th International Conference on Computer Applications in Industry and Engineering, New Orleans, LA, October 13–15, 2014), https://vford.me/papers/Ford%20Siraj%20Machine%20Learning%20in%20Cyber%20Security%20final%20manuscript.pdf; and Yonghua Wang et al., "A Survey of Dynamic Spectrum Allocation Based on Reinforcement Learning Algorithms in Cognitive Radio Networks," *Artificial Intelligence Review* 51, no. 3 (March 2019): 491–506.

[34] Elsa B. Kania, "China's Strategic Arsenals in a New Era," *Bulletin of the Atomic Scientists* (website), April 20, 2018, https://thebulletin.org/2018/04/chinas-strategic-arsenals-in-a-new-era/.

[35] Tucker, "AI-Enabled Weapon."

[36] Polat Ceviket et al., "The Small and Silent Force Multiplier: A Swarm UAV—Electronic Attack," *Journal of Intelligent & Robotic Systems* 70, no. 1-4 (2013): 595–608.

[37] Amjad Rehman and Tanzila Saba, "Evaluation of Artificial Intelligent Techniques to Secure Information in Enterprises," *Artificial Intelligence Review* 42, no. 4 (December 2014): 1029–44.

[38] Marina Koren, "The Mystery of the 'SpaceBees' Just Got Even Weirder," *Atlantic* (website), May 17, 2018, www.theatlantic.com/technology/archive/2018/05/rogue-satellites-launch-fcc/555482/.

Robotic systems are great for space warfare; they do not need life-sustaining equipment, which makes them less costly.[39] Space-based robots could be used to attack or collect information on adversarial satellites.[40] Multiple space-based robots could maneuver space debris into an orbit to hit adversary satellites or mount distributed, coordinated attacks.[41] Of course, a space-based swarm may have different technological challenges than a terrestrial swarm—especially successful movement and coordination.

More AI and robots on the battlefield means more opportunities to accuse adversaries of violating nascent norms of autonomous weapons and, therefore, more opportunities to wage psychological warfare. Improvements to AI might counter some of this concern. One concern of activists is machine learning is known to be brittle because training data may be biased or otherwise incomplete. Enhanced testing and evaluation, synthetic data, and data sharing may reduce the risks and provide opportunities for countermessaging. Judging how robust machine learning systems are would be difficult, if not impossible, without closely examining the training data. Adversaries may falsely claim the machine learning systems are untested and poorly designed, leading to high risks to civilians, and disproving such a claim would be extremely difficult, if not impossible. Thus, extensive deployment of these systems may lead to increased claims of violations of the laws of war.

## Policy Recommendations

The dependence of drone swarms on information warfare has several implications the military should consider for successful operations.

More in-depth studies of the relationship between drone swarms and information warfare are necessary and should explore the technical characteristics of informational interactions, how the information environment shapes tactical usage, and how tactical uses influence the operational and strategic environments. Some studies could perform modeling and simulation to assess the resilience of different drone-swarm configurations to informational attacks. Simulations and war games could explore the relative value of drone swarms in specific information-related roles (such as electronic attack) or as anti-satellite weapons.

[39] Peter W. Singer, "Op-Ed: Wired for War: The Future of Military Robots," Brookings Institution (website), August 28, 2009, https://www.brookings.edu/opinions/wired-for-war-the-future-of-military-robots/.

[40] Subrata Ghoshroy, "The X-37B: Backdoor Weaponization of Space?," *Bulletin of the Atomic Scientists* 71, no. 3 (2015).

[41] Marie Murphy, "70. Star Wars 2050," *US Army Training and Doctrine Command Mad Scientist Laboratory* (blog), July 23, 2018, https://madsciblog.tradoc.army.mil/70-star-wars-2050/.

Analysis should focus on how the information competition changes in different types of conflict (peer versus peer, peer versus near-peer, and asymmetric), the resilience of different forms of communication to electronic attack and how drone swarms fit into broader spectrum allocation, and new concepts incorporating drone swarms and how they interact with information warfare.

Research and development of friendly drone swarms must include hardening to informational attacks. Intraswarm communication channels, information processing systems, and longer-range, command-and-control systems must all be protected. Certain systems (such as object detection algorithms) will not be specific to swarms. Some promising research on information hardening has begun, such as the Defense Advanced Research Projects Agency's work on swarms that are operable in GNSS-denied environments.[42] These projects should be expanded. The degree to which a drone swarm is hardened should depend on the mission and the likelihood and type of information-based attacks the swarm may face.

The United States should also conduct a comprehensive review of information warfare capabilities across each service. Indications point to electronic-warfare challenges for the US Air Force and the US Army, though not the US Navy.[43] Major General John Morrison, commanding general of the US Army Cyber Center of Excellence, bluntly stated, "When it comes to electronic warfare, we are outgunned . . . We are plain outgunned by peer and near-peer competitors."[44] Recent reports also paint a negative image of military cybersecurity. An October 2018 Government Accountability Office report "found that from 2012 to 2017, [Department of Defense] testers routinely found mission-critical cyber vulnerabilities in nearly all weapon systems that were under development."[45] Department of Defense difficulties in recruiting cyberwarriors and a growing divide between Silicon Valley and the department exacerbate the challenge.[46] The United States faces increasing opposition in space, too. A recent unclassified Defense Intelligence Agency report found the following.

[42] Patrick Tucker, "The US Military's Drone Swarm Strategy Just Passed a Key Test," *Defense One* (website), November 21, 2018, www.defenseone.com/technology/2018/11/us-militarys-drone-swarm-strategy-just-passed-key-test/153007.

[43] Mike Pietrucha, "Low-Altitude Penetration and Electronic Warfare: Stuck on Denial, Part III," War on the Rocks, April 25, 2016, https://warontherocks.com/2016/04/low-altitude-penetration-stuck-on-denial-part-iii/; Sydney J. Freedberg Jr., "Army Tests Jamming MRAPs: New Electronic Warfare Vehicle," Breaking Defense, August 16, 2018, https://breakingdefense.com/2018/08/army-tests-jamming-mraps-new-electronic-warfare-vehicle/; and Mark Pomerleau, "US Is 'Outgunned' in Electronic Warfare Says Cyber Commander," *C4ISRNET* (website), August 10, 2017, www.c4isrnet.com/show-reporter/technet-augusta/2017/08/10/us-is-outgunned-in-electronic-warfare-says-cyber-commander/.

[44] Pomerleau, "US Is 'Outgunned.'"

[45] Cristina T. Chaplain, *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*, GAO-19-128 (Washington, DC: Government Accountability Office, October 2018).

[46] Amy Zegart and Kevin Childs, "The Divide between Silicon Valley and Washington Is a National-Security Threat," *Atlantic* (website), December 13, 2018, www.theatlantic.com/ideas/archive/2018/12/growing-gulf-between-silicon-valley-and-washington/577963/.

> Chinese and Russian military doctrines indicate that they view space as important to modern warfare and view counterspace capabilities as a means to reduce US and allied military effectiveness . . . Both have developed robust and capable space services, including space-based intelligence, surveillance, and reconnaissance . . . Both states are developing jamming and cyberspace capabilities, directed energy weapons, on-orbit capabilities, and ground-based antisatellite missiles that can achieve a range of reversible to nonreversible effects.[47]

The review should assess the true state of military information warfare and its alignment with adversarial developments, identify concrete recommendations to improve information warfare capabilities and organizations, and provide an unclassified set of recommendations and guidance for the defense industry and intelligentsia on how their efforts may support broader information warfare activities.

According to the review results, the US military would be able to make targeted investments in the study and development of offensive information warfare capabilities (for example, electronic jamming and offensive cyberweapons) to disrupt, manipulate, or otherwise defeat adversarial drone swarms that may be used against American forces. Such investments would also benefit other aspects of future warfare—from countering unmanned systems and information-dependent warfare concepts to disrupting adversarial supply chains.

Relevant capabilities should be integrated organizationally, and developments in robotics, electronic warfare, cyberwarfare, and space warfare should inform drone swarm acquisition, research and development, war gaming, concept and doctrine development, and related training. Activities should take place at the Joint level to the extent possible because the drone-swarm information challenge is the same for each service. Better integration across the components of the information domain would also be useful for nonswarming, unmanned systems because much of the analysis in this article also applies to them.

Intelligence collection on adversarial drone swarms and related information warfare aspects would be important, too. Intelligence collection aimed at drone-swarm technical operations would help the military understand how to manipulate or disrupt adversarial drone swarms and identify opportunities for covert action, such as poisoning data collections used for machine vision algorithms.[48] Other obvious targets for intelligence collections are adversarial

[47] Defense Intelligence Agency, *Challenges to Security in Space* (Washington, DC: Defense Intelligence Agency, 2019).

[48] Matthew Jagielski et al., "Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning" (working paper, 2018 Institute of Electrical and Electronics Engineers Symposium on Security and Privacy, San Francisco, California, May 21–23, 2018), https://arxiv.org/pdf/1804.00308.pdf.

organizations that combine information warfare capabilities (for example, the People's Liberation Army Strategic Support Force). Information gathered would help the military understand the capabilities potentially deployed against American and strategic partner drone swarms.

Before deploying a drone swarm, future commanders should evaluate the information warfare situation on the battlefield to inform the types of swarms to be used and their composition. For instance, commanders could include more communication drones to increase survivability. Training, exercises, and war games should be created to help commanders develop and exercise this judgment. In addition, incorporating information warfare elements into broader readiness and training activities would allow commanders to appreciate the challenges of losing control of the information environment. Commanders could also consider the deployment of counterelectronic warfare weapons to support the drone swarm in denied environments.

If the US military seeks to employ drone swarms in large numbers, it must also plan for the mitigation of the resultant psychological warfare risks and adopt measures to make these operations more transparent and to ensure appropriate human control, provided the transparency does not deliver advantages to adversaries. For example, the United States could adopt stronger restrictions on autonomous weapons by turning current restrictions under Department of Defense Directive 3000.09, *Autonomy in Weapon Systems*, into binding law or adopting new transparency policies on autonomous weapon capabilities.[49] These restrictions could be accompanied by costly commitments, such as investment in verification measures for autonomous weapons.[50]

## Conclusion

More than any other weapon system, drone swarms are dependent on information. Virtually every swarm-related capability requires mastery of information flows that let swarms grow in size, adopt complex behaviors, and operate in multiple domains simultaneously. These advantages, however, also pose a significant vulnerability. Disabling, disrupting, or manipulating swarm communication, information processing, and geolocation can disable or defeat a swarm.

No military technology exists in a vacuum. The military is a highly complex system of systems, and numerous technological areas are interdependent.

[49] "ICRC Position on Autonomous Weapon Systems," International Committee of the Red Cross (website), May 12, 2021, https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems.

[50] Matthew Mittelsteadt, *AI Verification: Mechanisms to Ensure AI Arms Control Compliance* (Washington, DC: Center for Security and Emerging Technology, February 2021).

Senior leaders must consider the role of new technologies within the broader military ecosystem because myopia and failure are fast friends.

Zachary Kallenborn

Zachary Kallenborn is a policy fellow at the Schar School of Policy and Government, a research affiliate of the Unconventional Weapons and Technology program at the National Consortium for the Study of Terrorism and Responses to Terrorism, a senior consultant at ABS Group, and officially proclaimed US Army "mad scientist." He is the author of publications on autonomous weapons, drone swarms, weapons of mass destruction, and terrorism involving weapons of mass destruction.

## Select Bibliography

Kallenborn, Zachary. *Are Drone Swarms Weapons of Mass Destruction?* Future Warfare Series no. 60. Maxwell Air Force Base, AL: US Air Force Center for Strategic Deterrence Studies, 2020.

Kallenborn, Zachary. "The Era of the Drone Swarm Is Coming, and We Need to Be Ready for It." Modern War Institute at West Point (website). October 25, 2018. https://mwi.usma.edu/era-drone-swarm-coming-need-ready/.

Krishna, C. G. Leela., and Robin R. Murphy, "A Review of Cybersecurity Vulnerabilities for Unmanned Aerial Vehicles." in *2017 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR)*. New York: Institute of Electrical and Electronics Engineers, 2017.

Michel, Arthur Holland. *Counter-Drone Systems*. Annandale-on-Hudson, NY: Center for the Study of the Drone, February 2018.

Scharre, Paul. "Counter-Swarm: A Guide to Defeating Robotic Swarms." War on the Rocks (website). March 31, 2015. https://warontherocks.com/2015/03/counter-swarm-a-guide-to-defeating-robotic-swarms/.

Theohary, Catherine A.. *Defense Primer: Information Operations*, IF10771. Washington, DC: Congressional Research Service, December 2020.

Verbruggen, Maaike. *The Question of Swarms Control: Challenges to Ensuring Human Control over Military Systems*. Non-Proliferation and Disarmament Paper no. 65. Brussels: EU Non-Proliferation and Disarmament Consortium, 2019.

Xi Chen, Jun Tang, and Songyang Lao, "Review of Unmanned Aerial Vehicle Swarm Communication Architectures and Routing Protocols." *Applied Sciences* 10, no. 10 (2020).