HSOAC | HOMELAND SECURITY OPERATIONAL ANALYSIS CENTER
An FFRDC operated by the RAND Corporation under contract with DHS

RESEARCH REPORT

DANIEL M. GERSTEIN, ERIN N. LEIDY

EMERGING TECHNOLOGY AND RISK ANALYSIS

Unmanned Aerial Systems Intelligent Swarm Technology

KEY FINDINGS

- Unmanned aerial systems (UASs), or drone technologies, for both individual systems and for surrogate swarms represent a current threat and, in the case of intelligent swarms, a growing threat given continued advances in range, payload, and power as UAS technology continues to mature.
- The maturing of intelligent swarms will come at the convergence of multiple technologies, including artificial intelligence, big data, Internet of Things, and fifth-generation cellular (5G), which will combine to support the development and employment of these capabilities.
- The risks of the illicit use of intelligent swarms will continue to grow over time; however, attacks will likely remain localized, with the potential for impacts to be felt regionally in some cases, such as cyber or electromagnetic attacks against the electrical grid. This would mean the consequences are likely to remain moderate because they are not likely to have a national impact.
- Vulnerabilities and consequences will likely be challenging to mitigate for homeland security defenders (e.g., law enforcement officers, first responders, planners, and workers in critical infrastructure sectors), because fielding detection systems and countermeasures across the range of potential targets could be extremely costly.

Unmanned aerial systems (UASs) or drone technologies, both individual systems and swarms of UASs, have proliferated over the past 25 years for a wide variety of applications. As a result, this technology and the ability to employ these UAS capabilities represent both a current and a growing threat as the technology continues to mature.

For this assessment, we delineate drone swarm technology into three categories: (1) multioperator-coordinated groups of individual drones; (2) drones that have been programmed in a coordinated manner to fly individually, in a leader-follower configuration, or in multidrone formations with a human operator controlling multiple drones; and (3) intelligent drone swarms that can communicate among individual drones and respond to external stimuli. The first two categories represent what we call in this assessment *surrogate* swarm technology, while the third category has been designated *intelligent* swarm technology.[1]

Swarm technology has already been demonstrated across a variety of civilian, law enforcement, and military uses. The technology for surrogate swarms should be considered readily available, but it does not have the same capability, agility, and flexibility as envisioned in intelligent swarm technologies that are being developed. As both individual UASs and surrogate swarm technologies continue to mature, it will become possible to deploy surrogate swarms in which individual swarm elements could communicate with each other or would be operated by a single individual in large-scale swarm flights with hundreds of drones covering hundreds of miles. Today, limiting physical factors for individual drones and surrogate swarms include the range, time of flight, and payloads; however, we expect that these system characteristics will continue to improve over time, allowing UASs to cover greater distances with higher payloads more efficiently.[2] As a result, both surrogate swarm categories could begin to approximate intelligent swarms of the future and already present a significant risk to the homeland.

The improvements in individual UASs and surrogate swarm technologies will translate into complementary improvements in intelligent swarm technology, which is the focus of our assessment. In our analysis of this technology, we consider four attributes: (1) technology availability (T_{AV}) and risks and scenarios (R_S), which we have divided into (2) threats, (3) vulnerabilities, and (4) consequences. The risks and scenarios have been provided by the study sponsors in the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and the Office of Policy. We compared these four attributes across three periods (see Figure 1).

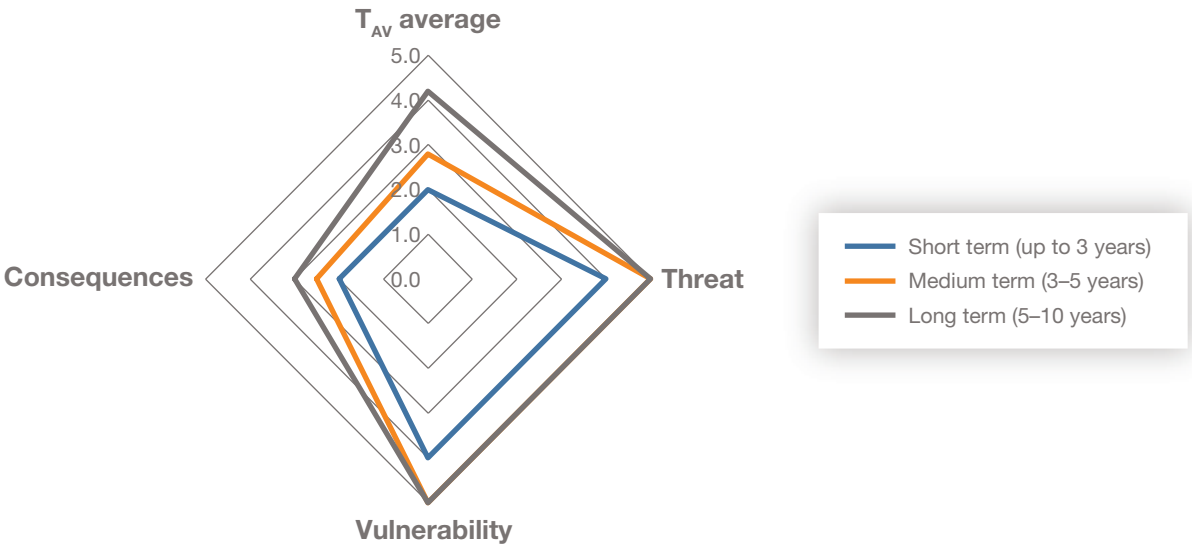
We assess the T_{AV} for intelligent swarm technologies should become readily available within the next five to ten years. In addition to coordination and communication between swarm elements, intelligent swarms will be able to respond to external stimuli, enabling greater capability for avoiding detection and being engaged and interdicted.[3] Additionally, the range, time of flight, and payloads are expected to continue to improve over the assessment period. However, the more sophisticated intelligent swarm technologies might not be available to all potential threat actors.

Regarding risks for the scenarios, we assess that threats and vulnerabilities are likely to peak in the medium term (three to five years), while consequences are likely to increase but reach only a moderate level. Vulnerabilities and consequences will likely be challenging to mitigate for homeland security defenders (e.g., law enforcement officers, first responders, planners, and workers in critical infrastructure sectors) because fielding detection systems and countermeasures across various potential targets could be extremely costly.

In evaluating the potential consequences, we assess that intelligent swarms could cause physical and non-

FIGURE 1

INTELLIGENT SWARM RISK ASSESSMENT



NOTE: Emerging technology risk assessment scale: 0 to < 2 = low impact or not likely feasible; 2 to < 4 = moderate impact or possible; and 4 to 5 = high impact or likely feasible.

kinetic outcomes that would produce local and perhaps even regional effects employing cyber or electromagnetic attacks against critical infrastructure. Even if the damaging results were localized or had minor impacts, the negative perception resulting from the perceived vulnerability and loss of well-being could raise the level of consequences.

Despite these challenges, we assess that fielding preparedness and response and mitigation measures could reduce vulnerabilities and consequences and, therefore, reduce the overall risk these intelligent swarm technologies will present.

TECHNOLOGY DESCRIPTION AND SCENARIOS FOR CONSIDERATION

A drone swarm consists of multiple UASs flying in a coordinated manner, which is either controlled remotely or self-controlled based on algorithms and programming that has been built into the systems.[4] Intelligent drone swarm technology also includes communications between drones within the swarm and the ability to respond to external stimuli.

Early UASs were developed more than 100 years ago, and the concept of employing drone swarms has been under consideration since small UASs have been in existence, with interest growing over the past 25 years. UASs are classified into five groups by the U.S. Department of Defense (DoD); the smallest Group 1 systems have a maximum gross takeoff weight of 0–20 pounds, a normal operating altitude of less than 1,200 feet above ground level (AGL), and an airspeed of less than 100 knots.[5] These Group 1 systems, in particular, are receiving the most attention for use in swarms. Group 2 UASs, with a maximum takeoff weight of 55 pounds, an operating altitude of less than 3,500 feet AGL, and an airspeed of less than 250 knots, could also be of concern for use in intelligent drone swarms. Both Groups 1 and 2 are covered under the Federal Aviation Administration's (FAA's) small UAS regulations (Part 107), which address all commercial-use UASs weighing less than 55 pounds.[6] While individual UASs and drone swarms have overlapping use cases and capabilities, the use of an intelligent swarm could provide benefits against detection and targeting of the individual drones at a reduced cost because these smaller drones are normally far less expensive than larger systems.[7]

For this assessment, we considered the terrorist use of an intelligent drone swarm equipped with explosives for attacking critical infrastructure as our primary scenario. Excursions from this scenario include the use of a swarm armed with explosives targeting a mass gathering, a drone swarm with cyber or electromagnetic attack capability employed against an electrical power substation, and a drone swarm being used by smugglers for conducting reconnaissance to avoid border patrols.

METHODOLOGY

We developed a framework for assessing the risks of emerging technologies. Our assessment included an evaluation of the T_{AV} and potential R_S for which a technology could be used. The T_{AV} evaluation included five areas: science and technology maturity; use case, demand, and market forces; resources committed; policy, legal, ethical, and regulatory impediments; and technology accessibility.[8] The R_S evaluation included threat, vulnerability, and consequences. The ratings for the T_{AV} and R_S categories range from 1 to 5, where 1 corresponds to many challenges and 5 to very few, if any, challenges. The ratings for the five T_{AV} areas were averaged and entered in the emerging technology risk framework. To allow for comparisons between different emerging technologies in assessing consequences, we rated impacts according to likely affected level (national, 5; regional, 4; and local, 1–3), along with considering mortality and morbidity likely totals, which could cause the rating to increase depending on

ABBREVIATIONS

5G	fifth-generation cellular
AI	artificial intelligence
COTS	commercial off-the-shelf
C-UAS	counter–unmanned aerial system
DARPA	Defense Advanced Research Projects Agency
DHS	U.S. Department of Homeland Security
DoD	U.S. Department of Defense
FAA	Federal Aviation Administration
IoT	Internet of Things
RCS	radar cross-section
R&D	research and development
R_S	risks and scenarios
S&T	Science and Technology Directorate
T_{AV}	technology availability
UAS	unmanned aerial system

the severity of the outcome. By averaging the ratings for threat, vulnerability, and consequences with the T_{AV} average calculated previously, we could assess the emerging technology risk for a particular scenario as low (0 to less than 2), moderate (2 to less than 4), or high (4 to 5).

We repeated these assessments for three periods: short term (up to three years), medium term (three to five years), and long term (five to ten years). This allowed us to assess individually and collectively how the T_{AV} and R_S would be affected over time. Our assessment considered how threats, vulnerabilities, and consequences evolved over time and whether preparedness or mitigation and response activities had been undertaken that could reduce the risk.

TECHNOLOGY AVAILABILITY ASSESSMENT

We assess that UASs or drone technologies for both individual systems and for surrogate swarms represent a current threat and, in the case of intelligent swarms, a growing threat given continued advances in range, payload, and power as UAS technology continues to mature.

The T_{AV} assessment is conducted without regard to the specific risks and scenarios. Those factors will be considered in the risk and scenario assessment section of this analysis. This is done to isolate the effects of the changes in technology over the ten-year study time frame.

In conducting this drone swarm assessment, we considered previous uses of drone swarm technology. For example, the U.S. military employed UAS surrogate swarm technology more than 20 years ago in the early stages of operations in Afghanistan. U.S. special operations forces employed swarm concepts using multiple drones, each controlled by an individual operator, to swarm against a target in a coordinated fashion.[9] Another example of drone swarms for nonmilitary purposes has been in laser light shows, where the movements have been synchronized and choreographed; however, these systems are not networked together and cannot make real-time decisions or respond to external stimuli.[10] By way of a final example, in Ukraine in 2022, Russia attacked targets using swarms of inexpensive "kamikaze" drones loaded with explosives sent in groups numbering in the low dozens, although once again each was not controlled by a single operator. Each of these cases represents *surrogate* swarm technology rather than the intelligent swarm technology that is being developed for future military and civilian applications.

SCIENCE AND TECHNOLOGY MATURITY

RAND research from 2005 defines surrogate drone swarming as "several units conduct[ing] a convergent attack on a target from multiple axes."[11] Therefore, we assess the drone swarm science and technology maturity level of UASs operated in swarm-like deployments as very high because surrogate swarms have been used in operational environments for the past 20 years. However, these relatively early uses of swarm technology do not provide a full picture of the capacity of drone swarms in the future.

In considering such future capabilities, one account describes swarm technology as follows: "a single operator from the ground can control hundreds of drones which can fly hundreds of [kilometers]. They have capabilities to carry payloads of 1 [kilogram] each. They can spend about an hour on target mission."[12]

Future intelligent swarms will come at the intersection of multiple technologies, including artificial intelligence (AI), big data, and the Internet of Things (IoT).[13] Additionally, they will be aided by the continued deployment of fifth-generation cellular (5G) communications technology (and future generations of cellular communications), as well as the emerging availability of radio frequency and satellite communications in locations where swarm technology will be employed.

Several DoD organizations, as well as international partners and potential adversaries, continue to experiment with intelligent swarm technologies. For example, in 2022, Defense Advanced Research Projects Agency (DARPA) testing demonstrated the use of a swarm of more than 150 drones controlled by a single operator. A DARPA official has predicted that within five years, a swarm may contain as many as 1,000 drones.[14] The U.S. Navy is looking to "build, deploy, and control thousands of small drones that are able to flock together to overwhelm anti-aircraft defenses with sheer numbers."[15] This same source highlights that "China, Russia, India, the [United Kingdom], Turkey, and Israel, which in 2021 became the first nation to use swarming drones in combat," are also pursuing these technologies. Once developed, these capabilities would be assessed at the highest technology readiness levels. If history is any indication, intelligent swarm technologies will proliferate rapidly into civilian applications that are already being discussed.[16]

To reach their full potential, drone swarms still need to overcome limitations associated with range, payload, and power. Indications are that UAS technology is continuing to mature and will likely overcome these current limitations by the end of the assessment period.[17] One way in which the military has mitigated these limitations

has been by deploying drone swarms in testing from a mother ship that releases the swarm in the vicinity of its intended target.[18] Such an approach could prove impractical for many terrorist organizations, but protecting against such an attack for high-priority targets could be considered to reduce risks. The maturing of intelligent swarm technology will come at the convergence of multiple technologies that will combine to support the development and employment of these capabilities.

USE CASE, DEMAND, AND MARKET FORCES

The previous "Science and Technology Maturity" section highlights how UAS technology is maturing and some of the use cases that are already envisioned for the future. As UAS individual and intelligent swarm technologies continue to mature, we expect additional use cases to be identified as the systems become more available and affordable. These use cases will pertain to civilian, military, and even illicit or nefarious actor applications.

Intelligent swarm technologies will enable more-capable systems with greater precision, less vulnerability, lower potential for collateral damage, and substantially lower costs. This will have important implications for militaries around the world; these same technologies will likely proliferate widely and rapidly to civilian applications. Already some of the potential civilian use cases cited include stage entertainment, hobbyist war games, search and rescue, spot spraying, animal herding, Wi-Fi coverage, national security, delivery of goods, and space exploration.[19]

Market forces are likely to increase as well, given expected advances in AI, big data, IoT, and 5G (and future generations of communications technology); this will likely result in increased proliferation of the technology. However, until 5G is fully deployed around the globe, some challenges for the use of swarm technology either for military or civilian purposes could be possible. Once 5G is widely available, we should expect to see greater demand for the technology and additional use cases identified.

These use cases will likely extend to nefarious actors (potentially including nations, terrorists, and criminals) who will look to use the technology to advance their objectives. Intelligent swarms could also provide flexibility in payloads and even mixed swarm payload capabilities. Such possibilities include carrying sensors, jammers, or other electronic warfare gear; surveillance sensors; and explosive warheads. Such actors will likely find the reduced vulnerability of their systems to countermeasures and, therefore, the greater chance of success of their attacks as reasons to pursue swarm technology. Some of these risks could involve the scenarios that are discussed later in the "Risk Assessment" section.

RESOURCES COMMITTED

The global swarm intelligence market is estimated to be valued at $447.2 million by 2030.[20] The growing size of the global market belies an opposite trend of the reduced cost of small UASs. As a result, swarm technology is likely "to overcome a fundamental problem of military hardware: cost."[21] Beyond military applications, drone swarm technologies will provide low-cost alternatives to conducting a variety of attack and reconnaissance scenarios that nefarious actors might find very attractive.

The actual commitment of funds would likely depend on the number of systems in a drone swarm, the range and payload, and whether any special engineering would be needed for a specific mission. For a majority of applications, commercial off-the-shelf (COTS) systems would likely be adequate, with modification required only for specific mission requirements, such as affixing explosive material or electromagnetic transmitters to the drones. The employment of an intelligent swarm depends on the convergence of multiple technologies, but these can likely be integrated from COTS systems as well (e.g., commercial 5G networks for command, control, and communications and 3D printers for printing specialized attachment parts).

POLICY, LEGAL, ETHICAL, AND REGULATORY IMPEDIMENTS

The FAA has regulations that cover drone operations and registration.[22] Small drones—like the type one would expect to see in a drone swarm—would be covered under Code of Federal Regulations, Title 14, Part 107, known as the FAA's small UAS regulations for most commercial applications for systems weighing less than 55 pounds.[23] For recreational use, compliance with Part 107 is not necessarily required. The FAA also has specific rules regarding use for "operations around people" that seek to safely integrate UASs into the National Airspace System.[24]

The FAA has already approved several waivers for drone swarms. In one case for use in agriculture, the waiver is known as "fly and apply" and pertains to rural areas. It allows for the capability to spray approximately 40 acres per hour, which nearly triples the current 14 acres per hour. The waivers are normally limited to specific geographical areas and are allowed in all 48 contiguous states.[25]

In 2019, Oklahoma State University was granted a certificate of authorization from the FAA for its Unmanned Systems Research Institute to "permit a single pilot, along

with visual observers for safety considerations, to operate a swarm of up to 20 fixed wing aircraft."[26] The application is for research and development (R&D) toward establishing "safe and efficient autonomous flight that will be common-place in years to come."[27]

More broadly, the FAA has regulations that limit and, in some cases, prohibit "operation of multiple small, unmanned aircraft" without receiving specific waivers, which was the case in the two examples cited previously.[28] As a result, some have argued that state and local law enforcement should be focusing on drone operators' compliance with FAA rules and regulations. However, these rules are difficult to enforce.

The 5G proliferation will also solve another technical problem regarding assured communications links for beyond visual line of sight (BVLOS) communications between the operator and the drone or drone swarm. While the use of an unlicensed radio frequency signal is susceptible to interference and spectrum crowding, 5G will solve that issue.[29] Still, it is worth noting that BVLOS UAS operations are currently prohibited by the FAA, with the exception of a very small number of waivers given primarily to government agencies.

Making illegal modifications to commercial systems would likely be beyond the technical capacity of an ordinary drone user, and FAA regulations prevent such modifications to be done without a waiver. It is worth noting that technologies that could be employed in an intelligent drone swarm are not likely to be export controlled unless they were solely for military applications. Overall, the policy, legal, ethical, and regulatory impediments do not present a significant barrier to overcome and, therefore, do not serve as a significant deterrent.

TECHNOLOGY ACCESSIBILITY

Over the next three years, UAS technology will continue to proliferate. While having an intelligent drone swarm that could be operated by a single person employing hundreds of drones over hundreds of kilometers is likely to remain challenging over the next three to five years, we should expect to see growing numbers of use cases in the future. The early uses in R&D, such as the Oklahoma State University study and agricultural application, highlight that this technology will continue to experience an increase in use. The low cost of the systems will make them attractive across a wide variety of applications.

There are few limitations, and those that are in place, such as the FAA limits on modifications of drone technology and flight rules, do not present significant barriers to technology accessibility, especially for actors seeking to use the technology for illicit purposes.

OVERALL TECHNOLOGY AVAILABILITY

While most of the use cases to date have been of surrogate or drone swarm–like capabilities, continued R&D should result in the technology maturing over the next three to five years. For our assessment, we have examined the *intelligent* swarm technologies versus the above-cited surrogate swarm capabilities. We expect that UAS technology will continue to mature along with, in particular, the enabling technologies of AI, big data, and IoT (used in conjunction with 5G). A corresponding increase in maturity of the intelligent swarm technology, as well as the democratization and deskilling of the technology, will likely ensue.

Table 1 provides our assessment for future intelligent drone swarm technologies in the short term, medium term, and long term. Just to reiterate, this assessment is for *intelligent* swarms, not drone swarm surrogates. Had this assessment been conducted for drone swarm surrogates in the short term, the **science and technology maturity**; **use case, demand, and market forces**; and **technology accessibility** would all have been rated as 5s, meaning there were few or no limitations. Recalculating the T_{AV} for surrogate swarm technologies in the short-term case would be a rating of 4, indicating that the technology would be available.

TABLE 1

INTELLIGENT SWARM TECHNOLOGY AVAILABILITY

Period	Science and Technology Maturity	Use Case, Demand, and Market Forces	Resources Committed	Policy, Legal, Ethical, and Regulatory Impediments	Technology Accessibility	T_{AV} Average
Short term (0–3 years)	3	1	3	2	1	2.0
Medium term (3–5 years)	4	3	3	2	2	2.8
Long term (5–10 years)	5	5	4	3	4	4.2

NOTE: T_{AV} rating scale: 0 to < 2 = low or not readily available; 2 to < 4 = moderate or potentially available; and 4 to 5 = high or available.

In evaluating the individual technology assessment categories for intelligent swarms, the **science and technology maturity** will continue to increase, and the technology will become more readily available over the study time frame. While testing and evaluation of intelligent swarm technology is continuing, only limited uses of the technology have occurred to date. We should expect this to change with both **science and technology maturity** and **use case, demand, and market forces** both reaching full maturity over the next decade. As the technology matures, more **resources** will likely be expended to procure these systems. We also expect that **policy, legal, ethical, and regulatory impediments** will be further reduced, but even currently, they are not significant obstacles to overcome. Finally, **technology accessibility** will continue to increase over the next decade; its initial rating of 1 is based on needing to increase **science and technology maturity** before being readily available. However, by the end of the assessment time frame, intelligent swarm technology should be quite **accessible**, which would result in an increase of its T_{AV} from 2.0 in the short term to 4.2 (high or available) in the long-term assessment.

RISK ASSESSMENT

While the previous T_{AV} assessment was conducted without regard to the specific risks and scenarios, in this section, we explicitly consider specific R_S. We consider the terrorist use of drones for attacking critical infrastructure using explosives as our primary scenario. Excursions from that scenario include the use of an intelligent swarm armed with explosives targeting a mass gathering, a swarm with a cyber or electromagnetic attack capability targeting an electrical power substation, and a swarm being employed by smugglers for conducting reconnaissance to avoid border patrols. It is important to stress that these risk assessments of intelligent swarms are sensitive to the scenarios that were considered (and the intent and capabilities of the threat actors); said another way, the risks could be far higher under certain derived scenarios (e.g., use of a biological weapon instead of a chemical-based explosive).

The risks of the illicit use of intelligent swarms will continue to grow over time; however, attacks will likely remain localized, with the potential for impacts to be felt regionally in some cases, such as cyber or electromagnetic attacks against the electrical grid. This would mean their consequences are likely to remain moderate because they would not likely have a national impact.

The risks of the illicit use of intelligent swarms will continue to grow over time; however, attacks will likely remain localized.

THREAT

The use of individual drones and drone swarm surrogates has proliferated for a variety of legal and illegal activities. For this assessment, we considered lone wolves and terrorist groups as threat actors. We assess that the ability to acquire and employ UASs and intelligent swarm technology will be related to the financing, sophistication, and planning capabilities of the actor; larger, well-financed groups are more likely to acquire and employ intelligent swarms initially. As the technology matures and becomes more widely available, even lone actors are more likely to gain access to intelligent swarm technology as described in the "Overall Technology Availability" section earlier. We also assess that the observed military uses in Iraq and Afghanistan by coalition partners and insurgents, coupled with more-recent operations by both Russia and Ukraine in that war, have illustrated use cases that could inform and embolden illicit actors in the homeland.

The surrogate swarm threat exists now and has been demonstrated on battlefields in Iraq and Afghanistan by insurgent forces against U.S. and coalition forces, and more recently by Ukrainian forces using a variety of drones and explosive devices against Russia. One account of the Ukrainian military's experience in using drones (both individually and in surrogate swarms) highlights the use of systems that include locally made lightweight R-18 quadcopters carrying former Soviet ordnance, such as grenades, to a TB-2 (a Turkish UAS) that could carry 1,500-pound missiles.[30] The drones have also been used in a variety of missions, such as surveillance, targeting, and bombing and firing missiles, and as cruise missiles.[31] Russia is also employing surrogate drone swarms, using Iran-provided attack drones against Ukrainian targets, particularly civilian infrastructure.[32] Terrorist groups, such as the Islamic State, have

already employed individual drones on the battlefield and could easily incorporate surrogate swarm techniques in their operations.

In assessing this threat, it is important to emphasize that these uses of drones are not intelligent swarms but rather collections of individual drones that have been programmed to follow flight plans and simultaneously attack a target or multiple targets.[33] In at least one foreign military operation highlighted previously, intelligent swarm technology has reportedly been employed (by U.S. forces in Afghanistan).

A 2020 Homeland Security Operational Analysis Center report highlights the potential uses of drone technology for attacks, including direct attack, indirect attack, diversion, and cyberattack, and for non-attack scenarios, including intelligence, surveillance, reconnaissance; passive collection; command, control, and communications; disruption; conveyance; and nuisance.[34]

Regardless of the current state of drones and drone swarm technologies, we should expect their proliferation to continue with increasing use of more-capable intelligent swarm technology. Threat actors will find this technology more readily available, and we should expect to see innovations in future use cases and effectiveness. In these types of scenarios, intelligent swarm technology will increase the effectiveness of the swarms while reducing the vulnerability of these systems to potential mitigations.

VULNERABILITY

Swarm technologies present a challenge for homeland security preparedness, response, and mitigation. Regardless of whether surrogate drone swarms or intelligent drone swarm technology is employed, the numbers of drones employed in these swarms will present challenges for developing and fielding countermeasures. These individual systems and the operational swarms can be outfitted with a variety of mission effect capabilities, from explosives and direct fire systems (such as guns or missiles) to jamming and even destructive electronic warfare.

While the U.S. military has been seeking to gain countermeasures against swarm technologies, with some in development, the number of individual drones that would need to be destroyed or rendered non–mission capable to mitigate this threat presents a challenge to be overcome. Recently, Ukraine has been using a Lithuanian-designed communications jammer called SkyWiper to defend against drones. An Israeli defense contractor has a system in development that hacks the guidance software of drones.[35] DoD has begun to invest in, and strategize about, counter-UAS (C-UAS) solutions as well.[36] Outside a military context, the S&T has also established a program to pilot and study C-UAS technologies.[37]

Still, their small size and use of nonmetallic materials, which reduce the radar cross-section (RCS) of these systems, make acquiring them at longer ranges a challenge, especially if one is employing techniques to evade detection. Systems today normally employ carbon fiber composites, which reduce the RCS, also confounding detection. In response, new detection systems using multi-spectral and light detection and ranging (LiDAR) sensors are being developed, but they are not fully mature yet.[38]

By way of an example, had the attacks against electrical substations in North Carolina in November 2022 incorporated intelligent swarms, the damage inflicted could have been greatly increased. Such an attack also provides a higher likelihood of success, given the challenges associated with destroying a large swarm. Additionally, the use of swarms would give the perpetrator of such an attack greater standoff distance.

The increased options for mission capabilities, challenges associated with destroying multiple small swarming drones, and increased accessibility to intelligent swarm technology will result in greater vulnerability to high-value targets in the homeland.

Swarm technologies present a challenge for homeland security preparedness, response, and mitigation.

CONSEQUENCES

In the “Vulnerability” section earlier, we alluded to the potential consequences of attacks against the homeland. In the 2022 North Carolina electrical substation attack, the use of explosives could have been far more catastrophic had an intelligent swarm been used to perpetrate the attack. Such catastrophic attacks could be kinetic or non-kinetic, using an electromagnetic attack, for example, and still result in significant damage to critical infrastructure.

A drone swarm being used against a mass gathering, such as a professional sports event, presents a special case. For example, one could envision the use of fuel air explosives in lieu of traditional explosives. Such an attack could be perpetrated at considerable standoff distances as discussed earlier.

Intelligent swarms having a greater capacity for evading detection and an ability to respond to external stimuli, coupled with the complexity of engaging numerous small targets, translate to increased risk with a higher likelihood of achieving their intended effects, whether that is destroying critical infrastructure or conducting reconnaissance.

EMERGING TECHNOLOGY ASSESSMENT

In the R_S assessment, we highlight that, whether a coordinated group of individual drones, surrogate drone swarms, or intelligent drone swarm technology is employed, the proliferation of the technology, demonstrated use cases by terrorists and insurgents in Iraq and Afghanistan, and the growing sophistication of its mission capabilities result in a growing risk and scenario concern.

In assessing such challenges, one account stated,

> It is difficult to detect, identify, classify, and—consequently—counter nefarious small unmanned aerial systems (sUASs) weighing less than 55 lbs, particularly in environments with high levels of sensory clutter, such as urban areas. As the U.S. Department of Homeland Security (DHS) prepares for potential threats from sUASs, it will need to know the types of threat scenarios in which these systems could be used, which design elements are likely to be exploited by a nefarious actor, and which technologies and capabilities may be available in the near future to either threaten public safety or facilitate DHS efforts to counter such activities.[39]

Drawing from available information on homeland security preparedness, we assessed mitigations that are being developed in response to these risks and scenarios (i.e., threats, vulnerabilities, or consequences). Table 2 provides an approximate risk assessment only that could be adjusted as additional information becomes available.

We assess that by the end of the long-term period (i.e., in the next five to ten years), each of the assessments for threat and vulnerability would be rated as a 5 for any of the mission packages that were considered. Ratings for consequences would range from 2 to 3 because we assess that such intelligent swarms would have predominantly state and local impacts, with the potential for regional impacts in the case of cyber or electromagnetic attacks against critical infrastructure, such as the electrical grid. The vast number of potential targets and their considerable risks to the homeland makes developing and deploying countermeasures extremely challenging. This, coupled with the advances in technology for intelligent swarms (as measured by a T_{AV} of 4.2), contributes to its being both high risk and a likely feasible threat, regardless of the mission package that is selected (e.g., explosives, jamming and electromagnetic attacks, reconnaissance). Of note, despite the emerging technology risk assessment rating of 3.8 overall in the medium term, placing it close to the likely feasible range, the T_{AV} rating of 2.8 for that period could be a limiting factor, moving this technology toward the merely possible range.

Additionally, for all three periods, the consequences have been rated as 3 or less, meaning they would be only moderate because their impacts would be at the local and potentially regional levels in the scenarios that we considered in the analysis. This assessment accounts for the localized impact expected from an attack of this type. It is possible that a regional impact could be felt should critical infrastructure be affected.

CONCLUSIONS

In analyzing the emerging technology of UASs through the risks and scenarios that were considered, we concluded that, whether surrogate drone swarms or intelligent drone

TABLE 2

INTELLIGENT SWARM RISK ASSESSMENT

Period	T_{AV} Average	Threat	Vulnerability	Consequence	Average Risk
Short term (up to 3 years)	2.0	4.0	4.0	2.0	3.0
Medium term (3–5 years)	2.8	5.0	5.0	2.5	3.8
Long term (5–10 years)	4.2	5.0	5.0	3.0	4.3

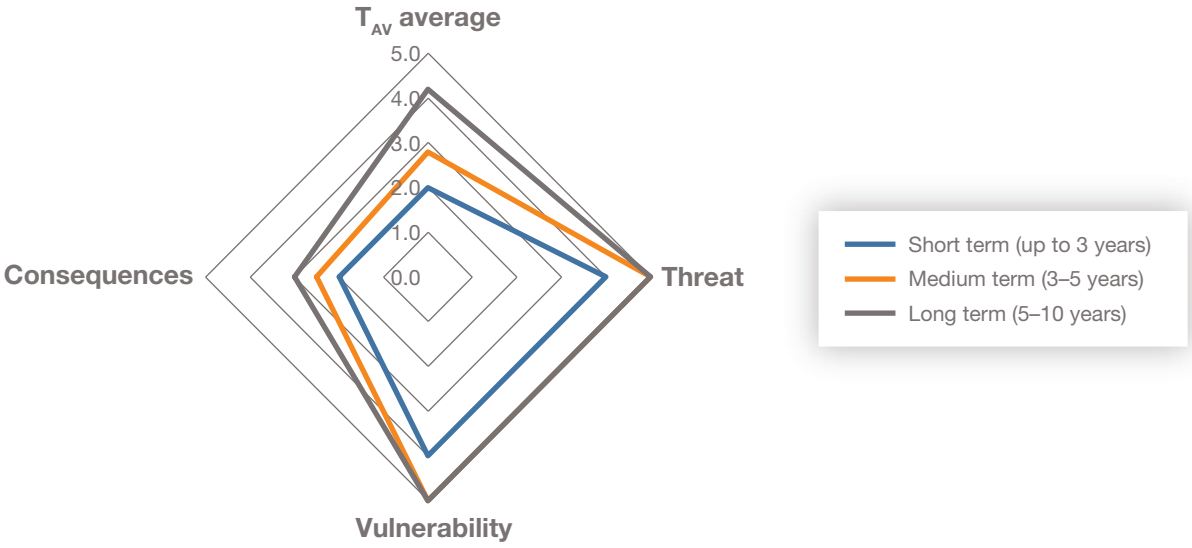
NOTE: Emerging technology risk assessment scale: 0 to < 2 = low impact or not likely feasible; 2 to < 4 = moderate impact or possible; and 4 to 5 = high impact or likely feasible.

swarm technology is employed, these systems present a significant risk to the homeland. The first two surrogate approaches—a coordinated group of individual drones and a surrogate drone swarm—could be achieved today. In assessing the long-term period, the science and technology maturity has increased, yet the relatively low score of the likely consequences translate to a moderate risk overall. Even if the damaging results are localized or have minor impacts, the negative perception resulting from the perceived vulnerability and loss of well-being could raise the level of consequences.

Finally, we assess that UAS technology—used either individually or in swarms—and its associated threats, vulnerabilities, and consequences will continue to increase. Vulnerabilities and consequences will likely be challenging to mitigate for homeland security defenders (e.g., law enforcement officers, first responders, planners, workers in critical infrastructure sectors) because fielding detection systems and countermeasures across the variety of potential targets could be extremely costly. Figure 2 again provides our overall risk assessment of this emerging technology by period.

FIGURE 2

INTELLIGENT SWARM RISK ASSESSMENT



NOTE: Emerging technology risk assessment scale: 0 to < 2 = low impact or not likely feasible; 2 to < 4 = moderate impact or possible; and 4 to 5 = high impact or likely feasible.

NOTES

1 Wilson et al., *Small Unmanned Aerial System Adversary Capabilities.*

2 Wilson et al., *Small Unmanned Aerial System Adversary Capabilities.*

3 Wilson et al., *Small Unmanned Aerial System Adversary Capabilities.*

4 RF Wireless World, "How Drone Swarm System Works/What Is Drone Swarm?"

5 Abdullah, "Geospatial Applications of Unmanned Aerial Systems (UAS)."

6 "FAA Rules and Regulations for Unmanned Aircraft Systems (UAS)."

7 RF Wireless World, "Advantages of Drone Swarm/Disadvantages of Drone Swarm."

8 This framework is described in Chapter 6 (pp. 143–62) and Appendix B (pp. 301–304) of Gerstein, *The Story of Technology.*

9 Arquilla and Ronfeldt, "Swarming—The Next Face of Battle."

10 Thorjussen and Samaritano, "Everything You Ever Wanted to Know About Drone Light Shows"; RF Wireless World, "How Drone Swarm System Works/What Is Drone Swarm?"

11 Edwards, *Swarming and the Future of Warfare.*

12 RF Wireless World, "How Drone Swarm System Works/What Is Drone Swarm?"

13 Wilson et al., *Small Unmanned Aerial System Adversary Capabilities.*

14 Pomerleau, "Contractors Demonstrate Single-User Drone Swarm at DARPA Experiment"; Harper, "Drone Swarms with 1,000 Unmanned Aircraft Could Be Possible Within 5 Years, DARPA Leader Says."

15 Hambling, "The US Navy Wants Swarms of Thousands of Small Drones."

16 Hambling, "The US Navy Wants Swarms of Thousands of Small Drones."

17 Wilson et al., *Small Unmanned Aerial System Adversary Capabilities.*

18 Hambling, "The US Navy Wants Swarms of Thousands of Small Drones."

19 Hambling, "The US Navy Wants Swarms of Thousands of Small Drones."

[20] Markets and Markets, "Swarm Intelligence Market."

[21] Hambling, "The US Navy Wants Swarms of Thousands of Small Drones."

[22] FlyLegit, "FAA Drone Registration."

[23] FAA, "Unmanned Aircraft System (UAS) or Drone Operations."

[24] FAA, "Operations over People General Overview."

[25] "FAA Approves Drone Swarms in Step Toward Automated Spraying Use."

[26] "OSA Receives First FAA Approval for Drone Swarm Operations in National Airspace."

[27] "OSA Receives First FAA Approval for Drone Swarm Operations in National Airspace."

[28] Rupprecht, "Section 107.35 Operation of Multiple Small Unmanned Aircraft."

[29] Gross, "Drone Swarms: Scaling Up for a New Level of Efficiency."

[30] Axe, "Ukrainian Drones Are Carpet-Bombing the Russians."

[31] Axe, "Ukrainian Drones Are Carpet-Bombing the Russians."

[32] Hambling, "Russia Is Now Using Iranian 'Swarming' Attack Drones in Ukraine—Here's What We Know."

[33] Pledger, "The Role of Drones in Future Terrorist Attacks."

[34] Wilson et al., *Small Unmanned Aerial System Adversary Capabilities*.

[35] Bowden, "The Tiny and Nightmarishly Efficient Future of Drone Warfare."

[36] DoD, *Counter-Small Unmanned Aircraft Systems Strategy*.

[37] DHS, "Countering Unmanned Aircraft Systems."

[38] Wilson et al., *Small Unmanned Aerial System Adversary Capabilities*.

[39] Wilson et al., *Small Unmanned Aerial System Adversary Capabilities*.

REFERENCES

Abdullah, Qassim A., "Geospatial Applications of Unmanned Aerial Systems (UAS)," Pennsylvania State University, College of Earth and Mineral Sciences, courseware module GEOG 892, undated. As of February 15, 2023: https://www.e-education.psu.edu/geog892/node/5

Arquilla, John, and David Ronfeldt, "Swarming—The Next Face of Battle," *RAND Blog*, September 29, 2003. As of February 15, 2023: https://www.rand.org/blog/2003/09/swarming----the-next-face-of-battle.html

Axe, David, "Ukrainian Drones Are Carpet-Bombing the Russians," *Forbes*, August 22, 2022.

Bowden, Mark, "The Tiny and Nightmarishly Efficient Future of Drone Warfare," *The Atlantic*, November 22, 2022.

DHS—*See* U.S. Department of Homeland Security.

DoD—*See* U.S. Department of Defense.

Edwards, Sean J. A., *Swarming and the Future of Warfare*, dissertation, Pardee RAND Graduate School, RAND Corporation, RGSD-189, 2005. As of February 15, 2023: https://www.rand.org/pubs/rgs_dissertations/RGSD189.html

FAA—*See* Federal Aviation Administration

"FAA Approves Drone Swarms in Step Toward Automated Spraying Use," *Spudman*, July 8, 2020.

"FAA Rules and Regulations for Unmanned Aircraft Systems (UAS)," *911 Security* blog, undated. As of February 15, 2023: https://www.911security.com/blog/faa-rules-and-regulations-for-unmanned-aircraft-systems-uas

Federal Aviation Administration, "Operations over People General Overview," webpage, last updated November 10, 2022. As of February 15, 2023: https://www.faa.gov/uas/commercial_operators/operations_over_people

Federal Aviation Administration, "Unmanned Aircraft System (UAS) or Drone Operations," webpage, last updated December 1, 2022. As of February 15, 2023: https://www.faa.gov/hazmat/air_carriers/operations/drones

FlyLegit, "FAA Drone Registration," webpage, undated. As of February 15, 2023: https://www.droneregistration.com/

Gerstein, Daniel M., *The Story of Technology: How We Got Here and What the Future Holds*, Prometheus Books, 2019.

Gross, Ben, "Drone Swarms: Scaling Up for a New Level of Efficiency," Elsight, August 24, 2022.

Hambling, David, "Russia Is Now Using Iranian 'Swarming' Attack Drones in Ukraine—Here's What We Know," *Forbes*, September 13, 2022.

Hambling, David, "The US Navy Wants Swarms of Thousands of Small Drones," *MIT Technology Review*, October 24, 2022.

Harper, Jon, "Drone Swarms with 1,000 Unmanned Aircraft Could Be Possible Within 5 Years, DARPA Leader Says," *FedScoop*, April 5, 2022.

Markets and Markets, "Swarm Intelligence Market," webpage, undated. As of February 15, 2023: https://www.marketsandmarkets.com/Market-Reports/swarm-intelligence-market-149256760.html

"OSA Receives First FAA Approval for Drone Swarm Operations in National Airspace," *Unmanned Airspace*, March 25, 2019.

Pledger, Thomas G., "The Role of Drones in Future Terrorist Attacks," Association of the United States Army, Land Warfare Paper 137, February 2021.

Pomerleau, Mark, "Contractors Demonstrate Single-User Drone Swarm at DARPA Experiment," C4ISRNET, January 20, 2022.

RF Wireless World, "Advantages of Drone Swarm/Disadvantages of Drone Swarm," webpage, undated. As of February 15, 2023: https://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-Drone-Swarm-Technology.html

RF Wireless World, "How Drone Swarm System Works/What Is Drone Swarm?" webpage, undated. As of February 15, 2023: https://www.rfwireless-world.com/Terminology/How-Drone-Swarm-System-Works.html

Rupprecht, Jonathan, "Section 107.35 Operation of Multiple Small Unmanned Aircraft," *Drone Law and Drone Attorney Assistance* blog, September 19, 2022.

Thorjussen, Nils, and Tony Samaritano, "Everything You Ever Wanted to Know About Drone Light Shows," Verge Aero, undated.

U.S. Department of Defense, *Counter-Small Unmanned Aircraft Systems Strategy*, January 2021.

U.S. Department of Homeland Security, "Countering Unmanned Aircraft Systems," November 2021.

Wilson, Bradley, Shane Tierney, Brendan Toland, Rachel M. Burns, Colby Peyton Steiner, Christopher Scott Adams, Michael Nixon, Raza Khan, Michelle D. Ziegler, Jan Osburg, and Ike Chang, *Small Unmanned Aerial System Adversary Capabilities*, Homeland Security Operational Analysis Center operated by the RAND Corporation, RR-3023-DHS, 2020. As of February 15, 2023: https://www.rand.org/pubs/research_reports/RR3023.html

ABOUT THIS REPORT

This report is part of a series of analyses on the effects of emerging technologies on DHS missions and capabilities. In this report, we examine unmanned aerial systems (UASs), or drone technologies, which represent both a current and a growing threat as the technology continues to mature, focusing our assessment on intelligent swarms of UASs. The Homeland Security Operational Analysis Center (HSOAC) was tasked with developing a technology risk assessment methodology for evaluating such emerging technologies and understanding their implications within a homeland security context.

This research was sponsored by the U.S. Department of Homeland Security (DHS) Science and Technology Directorate and conducted in the Management, Technology, and Capabilities Program of the RAND Homeland Security Research Division (HSRD), which operates HSOAC.

About the Authors

Daniel M. Gerstein is a senior policy researcher at the RAND Corporation. From 2011 to 2014, he served as the Acting Under Secretary and Deputy Under Secretary of the DHS Science and Technology Directorate. He has a doctorate in biodefense.

Erin N. Leidy is a technical analyst at the RAND Corporation and holds an M.S. in technology and policy. She has worked on data analysis and other support for a variety of military, homeland security, and national defense projects.

An FFRDC operated by the RAND Corporation under contract with DHS

The Homeland Security Act of 2002 authorizes the Secretary of the Department of Homeland Security (DHS), acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. The RAND Corporation operates the Homeland Security Operational Analysis Center (HSOAC) as an FFRDC for DHS under contract 70RSAT22D00000001.

The HSOAC FFRDC provides the government with independent and objective analyses and advice in core areas important to the Department in support of policy development, decisionmaking, alternative approaches, and new ideas on issues of significance. The HSOAC FFRDC also works with and supports other federal, state, local, tribal, and public- and private-sector organizations that make up the homeland security enterprise. The HSOAC FFRDC's research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under task order 70RSAT22FR0000125, Emerging Technology and Risk Analysis.

The information presented in this publication does not necessarily reflect official DHS opinion or policy.

For more information on HSRD, see www.rand.org/hsrd.

For more information on this publication, see www.rand.org/t/RRA2380-1.

This research was published in 2024.