B | Foreign Policy
at BROOKINGS

DEMOCRATIZING HARM: ARTIFICIAL INTELLIGENCE IN THE HANDS OF NONSTATE ACTORS

SARAH KREPS

NOVEMBER 2021

EXECUTIVE SUMMARY

Advances in artificial intelligence (AI) have lowered the barrier to entry for both its constructive and destructive uses. Just a few years ago, only highly resourced states and state-sponsored groups could develop and deploy AI-empowered drones, cyberattacks, or online information operations. Low-cost, commercial off-the-shelf AI means that a range of nonstate actors can increasingly adopt these technologies.

As the technology evolves and proliferates, democratic societies first need to understand the threat. Then they can formulate effective policy responses. This report helps them do both. It outlines the contours of AI advances by way of highlighting both the accessibility and appeal to nonstate actors such as terrorist, hacking, and drug trafficking groups. Based on the analysis, effective or feasible policy responses are unlikely to include outright bans on AI or autonomous vehicles that rely on AI because of questions about enforceability. AI is so diffuse that such bans are not practical and will not be effective. Instead, public-private partnerships will be key in incorporating software restrictions on commercial robotics, for example, which would address the potential consequences of nonstate actors using AI to program the flight and targeting of a drone.

Cultivating a broader and deeper talent pool in the science, technology, engineering, and math (STEM) fields will also help enrich the ability of democratic states to guard against the misuses of AI-enabled technology. Lastly, democratic societies should work together to develop ethical use norms, which may not preclude the misuse by nonstate actors but at least create guardrails that present obstacles to the export of harmful AI technologies from states to non-states and can shape the ways nonstate actors consider using these technologies.

INTRODUCTION

Access to artificial intelligence-empowered technology for national security and homeland defense has increasingly democratized. Countries such as the United States, Russia, China, and Israel have certainly pioneered these technologies. Israel's Iron Dome missile defense system has an AI function that is trained to detect incoming rounds that might threaten civilian populations or military facilities.[1] All of these countries are developing or already have AI-enabled autonomous systems on the ground, sea, or air.

Those technologies are diffusing quickly to less advanced states and even nonstate actors. Proliferation problems of the past, for example with nuclear weapons, were comparatively easy.

Developing nuclear weapons requires large volumes of financial and natural resources and considerable scientific expertise — the combination of which only a wealthy and capable state could afford. By comparison, AI technologies present a much greater threat, as they are easier to acquire and could give nonstate actors asymmetric advantages over states.

One reason that nonstate actors have not acquired nuclear weapons is that the associated technology is concentrated in the hands of powerful state actors that have strong incentives to prevent proliferation. AI-based technologies are not as capital-intensive as missiles or military bases, and they do not require specialized scientific knowledge to develop like nuclear weapons. Some AI algorithms are open source and therefore accessible and adaptable by a range of actors. Moreover, because the primary uses are not national security-related, AI development is driven more by the private sector and universities than governments. These civilian-developed AI-enabled technologies could therefore quickly proliferate among nonstate actors and even individuals.

The acquisition of AI-based technologies by nonstate actors threatens to destabilize existing state-nonstate dynamics on the battlefield.

The acquisition of AI-based technologies by nonstate actors threatens to destabilize existing state-nonstate dynamics on the battlefield. Nonstate actors have already deployed semi-autonomous drones that are inexpensive relative to the far costlier and more sophisticated weaponry of states. These actors can maneuver the drones to circumvent the boundaries of vehicle-borne threats, thereby maximizing the destructiveness and giving the actors an asymmetric advantage. Autonomous drones offer additional advantages, allowing nonstate users to preprogram drone activity to pursue particular types of targets in ways that make defense even more challenging. In cyberspace, accessible AI allows nonstate hacking groups to efficiently identify online vulnerabilities and attempt to extort financial resources from companies or individuals. In the information domain, AI enables nonstate actors to generate credible disinformation at scale, which can be used to manipulate a population group's views for political advantage.

As AI-enabled technologies proliferate among nonstate actors, democratic societies worldwide will need to understand fully how these actors may leverage these technologies. Only then can an effective response be formulated. To that end, this paper explores three applications of AI by nonstate actors, drawing on previous analyses of nonstate actors' acquisition of AI as well as priorities highlighted by reports such as that of the U.S. National Security Commission on Artificial Intelligence.[2] First, and most prominently, AI can be used to automate specific tasks such as sniping or drone strikes, which could target high-value individuals for assassination or minority groups within a country. Second, AI can be used to enable and maximize the impact of cyberattacks by leveraging machine learning of large datasets to prey on vulnerable individuals financially or psychologically. Third, AI can be used to employ algorithms to generate deepfakes or synthetic text to manipulate public opinion. For all three applications, the paper examines the technical underpinnings; the motivations; and the groups that have employed, or might consider employing these measures. Other analyses have pointed to the diffusion of AI-enabled surveillance and facial recognition technology,[3] but facial recognition can be incorporated into other technologies such as robotics so this paper does not consider it a separate category.

The paper then evaluates several potential policy responses. In doing so, it seeks to address a central question: what types of countermeasures exist to address the various contexts and ways in which nonstate actors use AI and dispel the potential asymmetric advantages? For example, AI regulation through an international organization is unlikely to be fruitful because the actors whose behaviors would be targeted are liable to be outside the organization's contours. Given this challenge, international efforts should focus on measures that impede the adverse consequences of AI-enabled technology, such as software restrictions programmed by drone manufacturers that limit where a drone can travel. Other efforts should include developing effective defensive instruments and forensics capabilities — in part through boosting the talent pool of domestic science, technology, engineering, and math (STEM) capabilities. Further, the establishment of ethical standards of use could then allow democratic societies to hold nonstate actors accountable when they misuse AI.

WHAT IS AI AND WHY DOES IT APPEAL TO NONSTATE ACTORS?

Artificial intelligence refers to "the ability of a machine to learn from experience, adjust to new inputs and perform human-like tasks."[4] The machine learns by processing large volumes of data, studying the successes and failures, and generating algorithms that help classify objects or predictions of behavior.[5] AI is frequently divided into two main types: weak (or narrow) and strong. Weak or narrow AI is the most common and is trained to perform specific, limited tasks. Voice assistants such as Alexa and Siri fall under this category. Strong AI, often called artificial general intelligence, typically involves more problem solving. The Roomba vacuum, for example, is trained specifically to clean a floor, but it has AI capabilities that allow it to survey the room size, identify obstacles, and remember efficient routes. However, it cannot go beyond the fairly repetitive motion for which it is trained or think to take a dirty dish and put it in the dishwasher.[6] Strong AI entails the range of analytics similar to humans, including a consciousness that allows individuals to solve problems, learn, and plan for the future, which is sometimes referred to as Super AI and is still speculative.[7]

Advancements in AI progress through two main pathways. One is through commercial development, which both introduces advancements and lowers the cost, thereby boosting accessibility. The commercial sector has been responsible for many of the technologies commonly associated with AI. Autonomous vehicles, for example, have received about 10% of the total global investment in AI ($7.7 billion), followed by the health sector (6%, about $4.7 billion), facial recognition (6%, about $4.7 billion), video content (4.5%, about $3.6 billion), and fraud detection and finance (3.9%, about $3.1 billion).[8] The U.S. defense sector, by comparison, was projected to spend $4 billion on AI research and development in 2020. As AI technology has progressed, the unit costs have decreased accordingly. A study of technical performance shows that the inference cost — that is, the cost in U.S. dollars to classify 10,000 validation images with an accuracy of greater than 93% — has declined precipitously in a short period, with the cost savings passed along to those who buy the technology.[9]

Alternatively, for AI that is not based on commercial developments but rather militaries, groups looking to acquire the technology must either steal the technology or import a relationship with one of the main producers.[10] AI development has been concentrated in relatively few countries. In terms of funding, the number of companies invested in AI, and the number of patents, the United States leads development, followed by China and the United Kingdom.[11] China has accelerated its investment in AI, however. In 2017, China accounted for 10% of global AI deals but Chinese AI start-ups attracted 48% of AI funding, which allowed it to surpass funding for U.S. AI start-ups that year (the U.S. had again attracted a majority of AI start-up funding in 2018).[12]

China's rising prominence in AI is notable because of the prospects for proliferation. A CNA report invoked China as a key Russian partner on AI. Both countries aim to maximize the impact of their joint investments in the face of American sanctions, export controls, and tariffs aimed to stifle innovation and competitiveness. At the center of the commercial collaboration is Huawei, which established its first research institute in Russia in 2017 with the intent to develop mathematical models for information technology and plans to triple its research and development staff in Russia. In 2020, the Huawei Russian Research Institute opened a lab to advance AI and deep learning and to leverage China's financial investments and Russia's talent pool.[13] China's AI collaboration with Russia is illustrative of its AI ambitions more generally. The mutual interest in collaborating resides in lowering the unit cost of technologies that can benefit each. A consequence of the collaboration, however, is the production of AI-enhanced technologies that can be exported more broadly to nonstate actors or sold via black markets.

The consequence of the decline in cost and rise in exportation of civilian-developed AI is a decrease in the barriers to entry. Whereas only advanced militaries can afford fighter aircraft, AI-enabled technology is becoming increasingly accessible in terms of both cost and availability to a range of nonstate actors.

The consequence of the decline in cost and rise in exportation of civilian-developed AI is a decrease in the barriers to entry. Whereas only advanced militaries can afford fighter aircraft, AI-enabled technology is becoming increasingly accessible in terms of both cost and availability to a range of nonstate actors.[14]

Nonstate actors are, definitionally, actors that are not tied directly to a government. In some settings, they include corporations, media organizations, and nongovernmental organizations such as Red Cross-style relief groups. In the context of nonstate actors and AI, this paper focuses on the types of actors that might engage in malicious behavior. The narrowest example is an individual. Cyber hackers, however, can conduct denial-of-service attacks or any number of hacks without necessarily being directed by an organization — just as individual lone wolves can conduct one-off terrorist attacks. Individuals with related interests can coalesce around more organized groups, such as the hacking group Anonymous that has been associated with conducting cyberattacks against governments. Even more organized nonstate actors include those with political objectives, terrorist groups, insurgencies, and militias and paramilitary groups.

AI's affordability and accessibility make the technology desirable to nonstate actors and enables them to overcome the resource and expertise disadvantages associated with operating outside the structure of a state. The state itself has, in principle, a monopoly over the use of force, and nonstate individuals and groups act outside the state to achieve their goals, such as politically undermining the state in which they operate or an adversarial state. Almost by definition, nonstate actors either have fewer resources or access to traditional military assets such as tanks, airplanes, or advanced weaponry. Because of their asymmetries in resources and authority, nonstate actors need to find ways to do more with less to overcome their power disadvantages. AI provides a vehicle for overcoming those resource asymmetries.

AI acts as an enabling technology, in the same way that electricity powers a vehicle or the combustion engine accelerates a train.[15] Nonstate actors looking to make their malicious activities more efficient and targeted would therefore find AI useful. It has a multiplier effect on the results of nonstate actors' activities. For example, on the battlefield, even a somewhat rudimentary drone becomes more ruthlessly efficient when powered by AI. In cyberspace, hacker groups can more effectively trawl the internet for vulnerabilities with the help of AI, leaving targets more susceptible and upping the ante for the financial amounts extracted. In the information domain, AI-based natural language models can generate credible text for large-scale disinformation campaigns that either persuade the target population to believe falsehoods or convince them to distrust media content as a general principle. The next section walks through these three categories of AI applications in more detail, grounding the intersection of AI and nonstate actor goals in a discussion of how AI enhances the core technologies and what types of actors have employed, or would be inclined to employ, the technologies.

AI TECHNOLOGIES AND THEIR UTILITY TO NONSTATE ACTORS

Nonstate actors continue to gain access to new AI-enabled weapons on the battlefield, in cyberspace, and in the information domain; and with this access, they gain new asymmetric ways of threatening state actors. Below are some examples of these affordances as well as insights on the recent and potential negative impacts.

AI-enabled battlefield advances

In the last decade, the use of armed drones on the battlefield has proliferated. The United States has frequently used unpiloted aircraft for counterterrorism operations in places such as Pakistan, Somalia, and Yemen. The technology proved to have advantages because it meant that U.S. pilots would not be shot down — thereby contributing to the favorable view of drones in a domestic political context.[16] From a tactical perspective, drones had advantages because they could loiter for longer over targets and help minimize civilian casualties while pursuing high-level combatants. Other countries witnessed the apparent battlefield successes and benefits — more precision and less risk because of the pilotless aircraft — and began to seek and acquire armed drones as well. More than 100 militaries have used either armed or unarmed drones in the 20 years since the U.S. first used drones on the battlefield in 2001.[17]

As drone technology has proliferated and advanced, the potential for autonomy has continued to grow. Most drones on the battlefield operate with some autonomy. For example, a surveillance drone might be programmed to fly a particular route to pick up "pattern of life" features of a potential target. The surveillance aspect of the drone mission is autonomous, but as of this writing, no one has deployed a fully autonomous drone for engaging with a target. Instead, the autonomously-gathered intelligence provides inputs, and a human decides whether to attack.

A fully autonomous drone — which would not only fly autonomously but also decide on its own whether to engage targets it identifies — would rely on AI. The process of full autonomy would entail hand coding targets based on whether the individual or object is a combatant (and should be targeted) or a civilian (and therefore protected), and then training a model on this data to arrive at an algorithm that has learned the difference between a combatant and civilian. This machine learning process could result in devastating false positives (identifying a civilian as a combatant) or false negatives (identifying a combatant as a civilian). The more controversial outcome is the former, because it means innocent people being killed by a machine.

Even if the algorithm were perfect and capable of accurately identifying a civilian from a combatant 100% of the time, battlefield circumstances can be complex and situational. For example, an algorithm could be trained to identify and target an individual putting on a suicide vest. But what if a young girl happens to walk in close proximity at the time that the autonomous drone identifies this high-level individual (a scenario illustrated in the movie "Eye in the Sky")? Programming the algorithm to anticipate every possible scenario is virtually impossible. An algorithm can be programmed to call off a strike when it sees a young person within a 25-meter radius, but how does the algorithm guide the drone if the young person is carrying a weapon or the target is preparing to target a school of young people? International humanitarian law indicates that civilian casualties should not be in excess of the military gain of the target, but there is no number or definition or threshold of proportionality; the threshold depends on a multitude of circumstances that cannot each be programmed into an algorithm.

The development of autonomous weapons systems using AI continues to accelerate, and some experts suggest that the U.S. should not sign onto a blanket prohibition against them because if Russia and China deploy fully autonomous systems, the U.S. will be at a disadvantage and should be willing to adopt these systems as well.

Because of the inherent risks, countries such as the U.S. and U.K. have stated that they would not make a first move toward full autonomy. However, the development of autonomous weapons systems using AI continues to accelerate, and some experts suggest that the U.S. should not sign onto a blanket prohibition against them because if Russia and China deploy fully autonomous systems, the U.S. will be at a disadvantage and should be willing to adopt these systems as well.[18] Russia reportedly recognizes the ethical pitfalls of using fully autonomous systems that not only conduct surveillance but targeting without human intervention but deems the systems to be inevitable.[19]

Thus far, state actors appear to be using drones in semi-autonomous ways, using autonomous systems that do not conduct lethal targeting, and developing systems that could in the future be involved in a range of autonomous missions. Iran, for example, used drone swarms to target Saudi Arabia's oil installations in 2019, literally flying below the radar of Saudi missile defense systems oriented toward higher-flying airborne vehicles.[20] In addition, China is developing AI-driven unmanned submarines that would conduct attack missions, lay mines, and conduct surveillance. The ability to operate autonomously underwater is particularly important because of the difficulty of underwater communications. China has also planned an AI-run underwater base that would use autonomous submarines that could deploy further afield. The AI-powered vehicles simulate decisionmaking such as surveying and clearing minefields and, by using neural networks to study and understand the ocean environment, to automate targeting decisions underwater.[21]

In a different, recent context, Israel appears to have used an AI-assisted sniper rifle to target an Iranian nuclear scientist. Israel has long been suspected of assassinating Iranian nuclear scientists but in particular had allegedly been preoccupied with an individual named Mohsen Fakrizadeh, who was leading the Iranian efforts to develop nuclear bombs. Iran also recognized the vulnerability of Fakrizadeh and insulated him from risk, for example traveling in convoys that changed routes, timing, and vehicles to foil attacks. The Israelis considered remote-controlled machine guns but placement would be a challenge given size and weight and problems of concealment. A close-range assassination would require agents in the field, which also bore risks. Instead, the Israelis smuggled a machine gun and robot into Iran and positioned the assembled weapon, a machine gun attached to a robotic apparatus, in Iran. The artificial intelligence compensated for the time delay between the sniper and machine gun, and when the convoy drove by, the remote sniper fired, identifying Fakhrizadeh based on facial recognition technology. Ultimately, an individual operating remotely fired the shot, but most of the identification was guided by AI and the attack was carried out by "an intelligent satellite system" as the Iranian Islamic Revolutionary Guard Corps evidently labeled it.[22]

Notably, discussions about the degree of acceptable autonomy — from fully manned to fully autonomous — often focus on state actors and the question of how and whether autonomous systems will continue to proliferate at the state level. But the demonstrated appeal of, and rising investment in these technologes mean that the increased use of both drones and AI-enabled autonomous capabilities by nonstate actors is almost inevitable.

Nonstate actors have already begun using drones on the battlefield. An open-source study found 440 unique cases in which weaponized unmanned aerial vehicles were used by nonstate actors in attacks, with 99% of those incidents taking place between August 2016 and March 2020.[23] In 2017, the Islamic State group (IS) used a drone to drop an explosive on a residential complex in Iraq, which caused three injuries. The overwhelming majority of these attacks (433 out of 440) have been in the Middle East and North Africa.[24] The advantage for nonstate actors is asymmetric. IS has used drones prolifically. In Mosul, for example, the group was recorded as having flown 300 drone missions in just one month — of which one-third were armed strike missions. Whereas a U.S.-armed drone would cost $22,000, IS was using small quadcopters for $650.[25] Even in the semi-autonomous mode, the small commercial systems provide intelligence, surveillance, and reconnaissance for the nonstate group and effectively deny access to the airspace where IS uses those drones. As a U.S. special operations commander noted regarding the group's use of drones in Mosul, the "killer bees" degraded morale and gave the enemy an advantage tactically — all through commercially available drones.[26] In November 2021, a "booby-trapped drone" struck Iraqi Prime Minister Mustafa al-Kadhimi's residence, sparing Kadhimi himself but injuring seven security officers. The assassination attempt was allegedly the work of paramilitaries and reveals both the access and disruptiveness of these technologies in the hands of nonstate actors.[27]

The rudimentary technology the Islamic State group used to kill two Kurdish fighters and wound French soldiers in 2016[28] now looks woefully outdated compared to the current drones because of both the rapid pace of development and the growing number of import options. Historically, Israel and the United States have been the largest drone manufacturers. One study estimated that in mid-2017, exports from Israel — including to Azerbaijan, Germany, and Nigeria — constituted more than 60% of international drone exports over the previous three decades.[29] But exports from the United States were particularly significant because the country developed the most advanced armed drones (the Predator and Reaper), though it limited sales to members of the North Atlantic Treaty Organization (NATO).

In recent years, China has become a major manufacturer, selling its models to Iraq, Nigeria, Pakistan, Saudi Arabia, and the United Arab Emirates.[30] Turkey has also increased its sales of drones. In the 2010s, Turkish drones sold to foreign countries were field tested from Azerbaijan and Armenia to Libya to Syria.[31] The Turkish government has increased in its investment in the drone industry, which appears to be elevating Turkish drones — the more they are used to strategic effect in conflict, the more attractive they have become to potential importers.[32] As more countries have developed and exported drones, the technology has become both more sophisticated and less expensive. Nonstate actors that have already carried out drone strikes, such as the Islamic State group, represent the obvious market for the AI-powered drones discussed above.

In addition to enhancing drone capacity, AI could increase the automation and lethality of a number of different nonstate activities. Miles Brundage et. al. note that AI could convert currently high-skill tasks, such as sniping, into more mundane tasks.[33] A U.S. Army document on AI-powered battlefield weapons observes that "a variety of instructions, how-to videos and even off-the-shelf trained AI software is readily available online that can be easily adapted to available weapons."[34] Automated gun turrets are just one example. There are YouTube do-it-yourself videos on building automated turrets that use Raspberry Pi, a small programmable computer, to sense targets and fire munitions. These videos show the assembly of all commercially available or at home-manufactured products: the 3D printed turret, software programming, and ingenuity imported from an online tutorial.

Groups such as IS that operate outside the context of a legitimate state and use violence to meet their objectives have shown an inclination towards acquiring and using other technology such as drones and would find automating high-skill tasks such as sniping appealing. For example, they could employ AI to conduct assassinations of specific individuals or selective killings of ethnic groups. They could also use AI-powered drones to identify and target specific members of crowds or to coordinate swarms of drones that overwhelm air defenses and strike targets. [35] The engineering task of coordinating a swarm has presented challenges, but algorithms will likely help overcome them. Machine learning algorithms allow swarms to navigate tight spaces by giving each drone in the swarm an algorithm that allows it to learn both the environment but also the other drones in the swarm.[36]

A number of recent episodes highlight how AI-powered weapons could change the battlefield. Nonstate actors have historically used semi-autonomous drones, but a recent United Nations report highlighted the use of a drone capable of flying both in manual and autonomous mode by a state-affiliated group — an episode that proves nonstate actors are likely interested in the technology.[37] The report revealed that in March 2020 in Libya, U.N.-backed Government of National Accord (GNA) forces used a Turkish-made Kargu-2 quadcopter drone to attack Libyan National Army (LNA) targets. Intervening in the nearly decade-long U.N.-authorized mission, the Turkish government aided the GNA by sending soldiers as well as intelligence and drones. The report notes that the Turkish-made drone loiters and then uses real-time image processing to track and hit targets: "The lethal autonomous weapons systems were programmed to attack targets without requiring data connectivity between the operator and the munition: in effect, a true 'fire, forget and find' capability."[38]

The report is ambiguous on whether the drone actually fired on a target in its autonomous mode and indeed the lack of clarity on this front foreshadows the problem of regulation that will be discussed later. The quadcopter looks innocuous and the ability to operate in two modes makes it difficult to discern how it was used. What is clear, however, is that the drone is fairly rudimentary yet potentially both lethal and autonomous. GNA is not technically a nonstate actor, but the Libyan state has been fractured for quite some time and the example is suggestive of how less capacious actors such as nonstate groups could both acquire and deploy a fully autonomous drone on the battlefield.

Similarly, Hamas has used small autonomous underwater drones, guided by GPS and carrying explosives, to try to attack targets in Israel, although the Israeli Navy appears to have destroyed these autonomous underwater vehicles. On the other hand, Israel also took a natural gas rig offline, in part an admission of the difficulty of defending against these new autonomous submarines.[39]

Drones have also become a platform of choice for drug cartels looking to transport illicit substances, conduct surveillance on enemies, or kill competitors. As Tim Bennett of the Department of Homeland Security's Science and Technology Directorate has observed, narcodrones are "a big new problem that we all have to address."[40] Drones that cost $5,000 can carry a payload of about 35 pounds, which can make the targeted delivery of drugs or the delivery of explosives more efficient. Surveillance drone footage could be analyzed through machine learning to understand open and closed routes, patterns of patrolling behavior, and efficient smuggling routes. Fully autonomous AI-powered systems could allow narcodrones to identify and target customs and border patrol agents to clear an unobstructed path, augmenting the insidiousness and lethality of trafficking operations.

Cyberattacks

Cyberspace is a second domain where AI is enabling capabilities that could become dangerous in the hands of nonstate actors. These actors carry out the majority of cyberattacks, whether for themselves or for a state that does not want to disclose its sponsorship. Groups of actors operating in cyberspace have various objectives. Politically motivated terrorist groups, for example, use cyber to effect political change by intimidating other audiences and recruiting and radicalizing like-minded individuals through propaganda. Jihadi groups use social media to distribute their ideology and coordinate attacks; for instance, the Islamic State group used Telegram to coordinate the November 2015 Paris attacks and March 2016 Brussels bombings.[41]

Hacktivist groups — with varying degrees of formality — use cyber to catalyze political, social, or cultural changes. For example, the group Anonymous has targeted religious groups, corporations, right-wing conspiracy theorists, and internet predators; most recently, it threatened entrepreneur Elon Musk over reckless tweets about cryptocurrency.[42] Mechanisms of attack include denial-of-service attacks that flood a website with traffic, for instance, and cause the site to crash.

Cybercriminals use this domain to exploit online user data for financial gain. Sometimes they employ spearphishing to steal data and then sell it; other times they use ransomware to hold a victim's information and then ask the individual for payment to regain access.[43] A recent example illustrates the potential allure for cybercriminal groups. In April 2021, a group called DarkSide was suspected of hacking Colonial Pipeline, which resulted in a shock to the availability of oil supply on the East Coast of the United States, and extorting millions in the equivalent cryptocurrency to restore supply.[44] The group, which was new but appeared to be composed of veteran cybercriminals, built on an increasingly prevalent approach of internet extortionism that links ransom payments with a key that in this case restored energy supply but in other cases can be the on/off switch to leaking confidential data such as medical records.[45] Digital extortionist groups not only generate income by threatening to leak data but also offer services to groups such as journalists to investigate leaked data.[46]

Effective cyberattacks hinge on finding the vulnerabilities in organizations... AI can help identify these markers and make cyberattacks cheaper to carry out, more accurate, more targeted, more automated, and more convincing.

Effective cyberattacks hinge on finding the vulnerabilities in organizations. Groups find these vulnerabilities in part by using applications that scan for weaknesses in computers, networks, and communications within a system. Outdated, unpatched, or misconfigured aspects of the system are markers of vulnerability. AI can help identify these markers and make cyberattacks cheaper to carry out, more accurate, more targeted, more automated, and more convincing. For instance, AI can help terrorists microtarget to maximize victims' potential receptiveness to their outreach efforts. In addition, hacktivist groups can use AI to shroud malicious code in innocuous applications, maximizing the impact of an attack by programming the code to execute when it finds the application most vulnerable. Lastly, groups that carry out phishing schemes to trick individuals into quickly and inadvertently granting their personal information can use AI to generate more tailored, convincing invitations.

Prototype-AI attacks are already here. Natural language models can study actual email threats to learn how to create — at scale — content that does not elicit suspicion. Phishing emails will often have a "please see attached" verbiage that is a flag for either spam filters or individuals. AI can craft emails that seem more credible and are more tailored to individuals, thereby helping to bypass filters and increase the likelihood of pernicious engagement that makes cyberoperations higher-yield.[47] AI may also be used by defense to identify and patch these vulnerabilities but cyberoperations are invariably a cat-and-mouse game and AI will continue to be used on offense to stay one step ahead and identify and target new vulnerabilities.[48]

Misinformation and disinformation

Misinformation, defined as "constituting a claim that contradicts common understanding of verifiable facts," and disinformation, which spreads that misinformation with an intention to deceive,[49] constitute a third domain where AI has the potential to empower and thus disrupt state actors. Both types of misleading content, whether the intent is to deceive or not, can polarize public opinion, and produce incivility and even violence. AI-enabled technologies can make it easier to write and distribute such content to manipulate opinion and public behavior. Natural language models train algorithms to write text that mimics the style and substance of the content on which it was trained. This technology has improved considerably, offering users the ability to generate credible news stories that could push disingenuous narratives — for example, through tweets that spout misinformation — and distort perceptions about the current or future political or social environment.[50]

Deepfakes work similarly using machine learning and neural networks to examine real facial expressions and movements and then create comparable fake but realistic images or video. Prominent people in the media, such as celebrities or politicians, are the usual targets of perpetrators because of the large volume of real images and videos needed to generate deepfakes. Deepfakes have already been made of politicians such as Speaker of the House Nancy Pelosi and former U.S. President Barack Obama.[51] Advances in AI — using neural networks to learn about language composition and facial structures — will only make natural language models and deepfakes even more convincing. To some extent, the concern with scaling up the manufacture of misleading content is pernicious whether or not individuals can discern the different. The proliferation of such content sows doubt in the media and contributes to cynicism toward democratic institutions if individuals no longer know what to believe.[52]

Nonstate actors could use synthetic text to manipulate the information environment in analogous ways and for nefarious ends. Terrorist groups in India, such as the Resistance Front and the Tehreeki-Milat-i-Islami group, have already used fake videos and photos to inflame groups, especially young people, and incite violence.[53] Terrorist groups have also set up fake charities to help finance their projects, as well as used doctored information as a recruiting tactic to boost morale. Advances in AI will enable even more sophisticated forms of online misinformation. For example, nonstate actors could use natural language models to generate videos that include messages from military authorities about attacking or retreating — to both manipulate the chain of command, and thereby events on the battlefield, and also public opinion. Such disinformation could put bottom-up pressure on civilian and military leaders to comport with the public's preferences.[54]

AI may also create even more targeted approaches to disinformation. As the 2016 U.S. presidential election showed, large volumes of data can be used in conjunction with machine learning to understand individual behaviors and preferences and then use algorithms to personalize ads meant to provoke or resonate with target audiences. AI enabled the microtargeting of swayable voters by using what the algorithms had learned of individual psychology.[55] In the 2016 election, it was the Russian Internet Research Agency that used AI-powered microtargeting, but nonstate actors can easily obtain these technologies from open-source markets. Thus, the number of actors manipulating media consumers will continue to grow, and over time, each actor will achieve ever-higher degrees of psychological finessing to do everything from shaping political preferences in an election to eroding public support for a war.

POTENTIAL COUNTERMEASURES

In 2017, Lieutenant General Paul Nakasone, then commander of the U.S. Army Cyber Command, observed that AI was being developed by the commercial sector rather than governments and that even small governments and nonstate actors would be "able to leverage that technology."[56] The sentiment has been echoed throughout the U.S. national security establishment. Mike Griffin, former undersecretary of defense for research and engineering, noted that "advances in artificial intelligence and global technology proliferation are driving the rapid evolution and global adoption of autonomy, which is creating economic, social and military disruption." Advancements in AI have led to the rapid diffusion across a wide range of actors, thereby creating enormous policy challenges.

One of the most aggressive proposed responses to AI proliferation has been an outright ban. But an all-out ban on AI is off the table because the civilian uses, such as for digital and writing assistants like Alexa and Google Smart Compose, are too ubiquitous. Bans on "unacceptable" uses of AI — defined as those "considered a clear threat to the safety, livelihoods and rights of people" — are designed to be more targeted (for example, to address facial recognition technologies) but are vague and therefore unlikely to succeed in stemming the development of AI technologies and their diffusion to nonstate actors.[57]

Calls for bans on specific applications of AI that might affect nonstate actors have become more common. One of the most visible proposals has been to regulate or ban lethal autonomous weapons; it is presented as the ethical approach for regulating these weapons.[58] In 2017, Elon Musk and physicist Stephen Hawking called for a ban on "killer robots," imploring the United Nations to ban both the development and use of AI-powered weapons.[59]

Despite the visibility of the proposals, talks at the United Nations have not made meaningful headway, with 28 governments proposing a ban on AI-powered autonomous weapons and the U.S. and Russia blocking legally binding agreements.[60] Even if an agreement were obtained, it would probably involve actors less likely to be responsible for lethal autonomous weapons, rendering the agreement relatively ineffective. For example, while Indian Prime Minister Narendra Modi has cautioned against the "weaponization of AI by nonstate actors," he has also stressed the need to continue developing AI and he clearly seeks to make India a global AI hub.[61] Modi's position on the issue reflects the contradiction inherent in many countries: they each desire to maintain these technologies while keeping them out of the hands of others, especially nonstate actors. Agreeing to a ban is something of a prisoner's dilemma. While all countries might benefit from a ban on the disruptive applications of autonomy, unless all countries agree to abide by it, there might be incentives to develop and use the technology first and not commit to a ban.

Many countries... view autonomous weapons as constructive... In the fog of war, where human operators are fatigued or emotional, human error may exceed that of an autonomous agent.

Further, many countries might rightfully view autonomous weapons as constructive and therefore oppose an outright ban on technologies that they might see as making war less inhumane. In the fog of war, where human operators are fatigued or emotional, human error may exceed that of an autonomous agent. Machines can also be incredibly adept at minimizing collateral damage. One of the remarkable features of the Fakhrizadeh assassination was that his wife, who was sitting next to him in the car, did not perish in the attack. The combination of the AI and the "electronic equipment" was sufficiently precise that it struck three to four individuals suspected to be involved in with the Iranian nuclear program but spared the scientist's wife, a civilian.[62]

One middle-ground proposal therefore reconciles the potential risk of autonomous systems for both states and nonstate actors with their potential for reducing the unfortunate consequences of either fogs of war, human error, or bluntness of conventional alternatives. Outright bans not only are not feasible but go too far and could have the unintended consequence of removing some of the technological advances that may minimize collateral damage on the battlefield. Instead, more prudent guardrails are in order. Private industry has a role to play in instituting measures that stem the proliferation of inexpensive off-the-shelf armed drones or at least their efficacy. For example, restrictions baked either into the hardware or software could prevent a drone from crossing certain boundaries — such as into a military base or the grounds of a national leader's residence.

Instituting norms and guiding principles about human involvement in the use of force, including humans making the ultimate decisions about lethal force, would also be advisable. The International Committee of the Red Cross (ICRC) has identified "a need for a genuinely human-centred approach to any use of these technologies in armed conflict. It will be essential to preserve human control and judgment in applications of AI… especially where they pose risks to life." The ICRC concludes that "AI and machine-learning systems remain tools that must be used to serve human actors, and augment human decision-makers, not replace them."[63] Norms that emphasize the human in the loop about decisions of life and death respect the practical challenges of banning technology as a whole and the potential for AI to reduce civilian casualties, though they need to be reinforced through state behavior and even then of course cannot be guaranteed to be followed by nonstate actors.

Somewhat different concerns arise about regulating or restricting the use of AI to spread disinformation. Determining what constitutes disinformation presents challenges, and as social media platforms have shown, identifying and removing all disinformation is a reactive response. In taking a more proactive approach, the U.S. National Security Commission on Artificial Intelligence has proposed draft legislation that would "detail how adversarial state and nonstate actors are attempting to define and control the global information domain to shape global opinion and achieve strategic advantage."[64] The proposal is mindful of the challenges of finding and removing content and takes more agency over the landscape into which these nonstate actors might insinuate themselves. By comparison, more aggressive approaches consist of legal measures against states that appear to be either sponsoring or tacitly allowing nonstate actors to operate within their borders — such measures would include requesting that the state take legal action, introducing economic sanctions, or indicting the malicious actor or group.[65]

A solution may also reside in measures democratic societies are taking to be technologically competitive anyway, which is to commit more resources to research and development in the science, technology, engineering, and math fields. In 2021, for example, the U.S. Senate voted 68-30 in favor of the United States Innovation and Competitiveness Act, which would authorize $190 billion to strengthen U.S. technology capabilities, which could have the dual purpose of helping to identify and guard against the use of AI-enabled offensive technologies in the hands of nonstate actors.[66] To the extent that these threats emerge from the commercial, non-military sector, preventing their diffusion will be an uphill battle. Mapping the terrain and the potential threats, as this report begins to do, is at least a first step toward framing questions whose answers will ultimately lead to impactful policy responses.

REFERENCES

1 Jim Garamone, "Esper Sees Iron Dome Missile Defense System in Tel Aviv," U.S. Department of Defense, October 30, 2020, https://www.defense.gov/News/News-Stories/Article/Article/2400629/esper-sees-iron-dome-missile-defense-system-in-tel-aviv/.

2 Eric Schmidt, Robert Work, Safra Catz, Steve Chien, Mignon Clyburn, Chris Darby, Kenneth Ford, José-Marie Griffiths, Eric Horvitz, Andrew Jassy, Gilman Louie, William Mark, Jason Matheny, Katharina McFarland, Andrew Moore, "Final Report," (Washington, DC: National Security Commission on Artificial Intelligence, 2021), 19, https://www.nscai.gov/2021-final-report/; Mark Pomerleau, "An edge for nonstate actors: AI," Fifth Domain, November 7, 2017, https://www.fifthdomain.com/international/2017/11/07/an-edge-for-non-state-actors-ai; T.X. Hammes, "Technology Converges; Non-State Actors Benefit," (Stanford, CA: Hoover Institution, February 25, 2019), https://www.hoover.org/research/technology-converges-non-state-actors-benefit.

3 Paige Young, "Artificial Intelligence: A Non-State Actor's New Friend," Over the Horizon, May 1, 2019, https://othjournal.com/2019/05/01/artificial-intelligence-a-non-state-actors-new-best-friend/.

4 Yanqing Duan, John Edwards, and Yogesh Dwivedi, "Artificial intelligence for decision making in the era of Big Data – evolution, challenges and research agenda," *International Journal of Information Management* 48 (October 2019): 63-71, https://www.sciencedirect.com/science/article/abs/pii/S0268401219300581.

5 "Artificial Intelligence," IBM, June 3, 2020, https://www.ibm.com/cloud/learn/what-is-artificial-intelligence.

6 Will Knight, "These Robots Use AI to Learn How to Clean Your House," *Wired*, September 30, 2020, https://www.wired.com/story/robots-use-ai-learn-clean-your-house.

7 "Strong AI," IBM, August 31, 2020, https://www.ibm.com/cloud/learn/strong-ai.

8 Raymond Perrault, Yoav Shoham, Erik Brynjolfsson, Jack Clark, John Etchemendy, Barbara Grosz, Terah Lyons, James Manyika, Saurabh Mishra, and Juan Carlos Niebles, "The AI Index 2019 Annual Report," (Stanford, CA: Human-Centered Artificial Intelligence, Stanford University, December 2019), 6, 90 https://hai.stanford.edu/sites/default/files/ai_index_2019_report.pdf.

9 Ibid, 210.

10 Michael Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review* 1, no. 3 (May 2018): 39, https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power.

11 Louise Lucas and Richard Waters, "China and US compete to dominate big data," *Financial Times*, Aptil 30, 2018, https://www.ft.com/content/e33a6994-447e-11e8-93cf-67ac3a6482fd.

12 "China Is Starting to Edge Out the US in AI Investment," CB Insights, February 12, 2019, https://www.cbinsights.com/research/china-artificial-intelligence-investment-startups-tech.

13 Jeffrey Edmonds, Samuel Bendett, Anya Fink, Mary Chestnut, Dmitry Gorenburg, Michael Korman, Kasey Stricklin, and Julian Waller, "Artificial Intelligence and Autonomy in Russia," (Arlington, VA: CNA, May 2021), 159-160, https://www.cna.org/centers/cna/sppp/rsp/russia-ai.

14 T.X. Hammes, “Technology Converges; Non-State Actors Benefit.”

15 Michael Horowitz, “Artificial Intelligence, International Competition, and the Balance of Power,” 37.

16 John Kaag and Sarah Kreps, *Drone Warfare* (New York: Polity, 2014), https://www.amazon.com/Drone-Warfare-Conflict-Modern-World/dp/0745680992.

17 Dan Gettinger, “Weapons of the future: Trends in drone proliferation,” *Defense News*, May 25, 2001, https://www.defensenews.com/opinion/commentary/2021/05/25/weapons-of-the-future-trends-in-drone-proliferation.

18 The National Security Commission for Artificial Intelligence argued that the U.S. and its allies should not be part of a global ban on AI-enabled autonomous weapons systems. See the commission’s final report, Eric Schmidt, Robert Work, Safra Catz, Steve Chien, Mignon Clyburn, Chris Darby, Kenneth Ford, José-Marie Griffiths, Eric Horvitz, Andrew Jassy, Gilman Louie, William Mark, Jason Matheny, Katharina McFarland, Andrew Moore, “Final Report.”

19 Jeffrey Edmonds, Samuel Bendett, Anya Fink, Mary Chestnut, Dmitry Gorenburg, Michael Korman, Kasey Stricklin, and Julian Waller, “Artificial Intelligence and Autonomy in Russia,” 80.

20 Seth J. Frantzman, “Are air defense systems ready to confront drone swarms?” *Defense News*, September 26, 2019, https://www.defensenews.com/global/mideast-africa/2019/09/26/are-air-defense-systems-ready-to-confront-drone-swarms/.

21 Leonardo Zacchini, Alessandro Ridolfi, Alberto Topini, Nicola Secciani, Alessandro Bucci, Edoardo Topini, and Benedetto Allotta, “Deep Learning for on-board AUV Automatic Target Recognition for Optical and Acoustic Imagery,” *IFAC-PapersOnLine* 53, no. 2 (2020): 14589-14594, https://www.sciencedirect.com/science/article/pii/S2405896320318784; and JR Wilson, “Unmanned submarines seen as key to dominating the world’s oceans,” *Military and Aerospace Electronics*, October 15, 2019, https://www.militaryaerospace.com/unmanned/article/14068665/unmanned-underwater-vehicles-uuv-artificial-intelligence.

22 Ronen Bergman and Farnaz Fassihi, “The Scientist and the A.I.-Assisted, Remote-Control Killing Machine,” *The New York Times*, September 18, 2021, https://www.nytimes.com/2021/09/18/world/middleeast/iran-nuclear-fakhrizadeh-assassination-israel.html.

23 Håvard Haugstvedt and Jan Otto Jacobsen, “Taking Fourth-Generation Warfare to the Skies? An Empirical Exploration of Non-State Actors’ Use of Weapnoized Unmanned Aerial Vehicles (UAVs — ‘Drones’),” *Perspectives on Terrorism* 14, no. 5 (October 2020): 30, https://www.jstor.org/stable/26940037.

24 Ibid.

25 Mark Pomerleau, “How $650 drones are creating problems in Iraq and Syria,” C4ISRNet, January 5, 2018, https://www.c4isrnet.com/unmanned/uas/2018/01/05/how-650-drones-are-creating-problems-in-iraq-and-syria.

26 Peter Layton, “Commercial drones: Privatising air power,” The Lowy Institute, September 27, 2017, https://www.lowyinstitute.org/the-interpreter/commercial-drones-privitising-air-power.

27 Ghassan Adnan and Jared Malsin, "Iraq's Prime Minister Targeted in Assassination Attempt," *The Wall Street Journa*l, November 7, 2021, https://www.wsj.com/articles/iraqs-prime-minister-survives-assassination-attempt-government-says-11636248485.

28 "Islamic State drone kills two Kurdish fighters, wounds two French soldiers," Reuters, October 11, 2016, https://www.reuters.com/article/us-france-iraq-iraq/islamic-state-drone-kills-two-kurdish-fighters-wounds-two-french-soldiers-idUSKCN12B2QI.

29 Elisa Catalano Ewers, Lauren Fish, Michael C. Horowitz, Alexandra Sander, and Paul Scharre, "Drone Proliferation: Policy Choices for the Trump Administration," (Washington, DC: Center for a New American Security, June 2017), http://drones.cnas.org/reports/drone-proliferation.

30 Peter Bergen, Melissa Salyk-Virk, and David Sterman, "Introduction: How we became a world of drones," in "World of Drones," (Washington, DC: New America, last updated July 30, 2020), https://www.newamerica.org/international-security/reports/world-drones/introduction-how-we-became-a-world-of-drones.

31 Sinan Tavsan, "Turkey begins to rival China in military drones," *Nikkei Asia*, October 7, 2020, https://asia.nikkei.com/Politics/International-relations/Turkey-begins-to-rival-China-in-military-drones.

32 Dan Gettinger, "Turkey's military drones: an export product that's disrupting NATO," *Bulletin of the Atomic Scientists*, December 6, 2019, https://thebulletin.org/2019/12/turkeys-military-drones-an-export-product-thats-disrupting-nato.

33 Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, Paul Scharre, Thomas Zeitzoff, Bobby Filar, Hyrum Anderson, Heather Roff, Gregory C. Allen, Jacob Steinhardt, Carrick Flynn, Seán Ó hÉigeartaigh, Simon Beard, Haydn Belfield, Sebastian Farquhar, Clare Lyle, Rebecca Crootof, Owain Evans, Michael Page, Joanna Bryson, Roman Yampolskiy, and Dario Amodeial, "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," (Oxford, U.K.: Future of Humanity Institute, University of Oxford, February 2018), 27, https://dataspace.princeton.edu/handle/88435/dsp01th83m203g.

34 Gordon Cooke, "Magic Bullets: The Future of Artificial Intelligence in Weapons Systems," U.S. Army, June 11, 2019, https://www.army.mil/article/223026/magic_bullets_the_future_of_artificial_intelligence_in_weapons_systems.

35 Miles Brundage, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, Paul Scharre, Thomas Zeitzoff, Bobby Filar, Hyrum Anderson, Heather Roff, Gregory C. Allen, Jacob Steinhardt, Carrick Flynn, Seán Ó hÉigeartaigh, Simon Beard, Haydn Belfield, Sebastian Farquhar, Clare Lyle, Rebecca Crootof, Owain Evans, Michael Page, Joanna Bryson, Roman Yampolskiy, and Dario Amodeial, "The Malicious Use of Artificial Intelligence," 21.

36 J. Fingas, "AI helps drone swarms navigate through crowded, unfamiliar spaces," Engadget, July 18, 2020, https://www.engadget.com/caltech-drone-swarm-ai-174642584.html.

37 "Final report of the Panel of Experts on Libya established pursuant to Security Council resolution 1973 (2011)," (New York: United Nations, March 8, 2021), https://digitallibrary.un.org/record/3905159?ln=en.

38 Ibid., 17.

39 Judah Ari Gross, “IDF says it thwarted underwater drone attack by Hamas from northern Gaza,” *Times of Israel*, May 18, 2021, https://www.timesofisrael.com/idf-says-it-thwarted-underwater-drone-attack-by-hamas-from-northern-gaza/.

40 Tim Wright, “How Many Drones Are Smuggling Drugs Across the U.S. Southern Border?” *Air & Space Magazine*, June 2020, https://www.airspacemag.com/flight-today/narcodrones-180974934.

41 Mia Bloom and Chelsea Daymon, “Assessing the Future Threat: ISIS’s Virtual Caliphate,” *Orbis* 62, no. 3 (2018): 372-388, https://www.sciencedirect.com/science/article/abs/pii/S0030438718300437.

42 Andy Gregory, “Anonymous accuses Elon Musk of ‘destroying lives’ with dryptocurrency tweets,” *The Independent*, June 6, 2021, https://www.independent.co.uk/life-style/gadgets-and-tech/elon-musk-anonymous-bitcoin-crypto-b1860458.html.

43 Lillian Ablon, “Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data,” (Congressional testimony, Washington, DC, March 15, 2018), https://www.rand.org/pubs/testimonies/CT490.html.

44 “Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside,” U.S. Department of Justice, June 7, 2021, https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

45 Raphael Satter, “Ransom group linked to Colonial Pipeline hack is new but experienced,” Reuters, May 10, 2021, https://www.reuters.com/business/energy/ransom-group-linked-colonial-pipeline-hack-is-new-experienced-2021-05-09.

46 “Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar,” (Washington, DC: Public-Private Analytic Exchange Program, U.S. Department of Homeland Security, 2019), 5, https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf.

47 William Dixon and Nicole Easgan, “3 Ways AI will change the nature of cyber attacks,” World Economic Forum, June 19, 2019, https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence.

48 “Artificial Intelligence as Security Solution and Weaponization by Hackers,” *CISOMAG*, December 9, 2019, https://cisomag.eccouncil.org/hackers-using-ai.

49 Andrew Guess and Benjamin Lyons, “Misinformation, Disinformation, and Online Propaganda,” in *Social Media and Democracy: The State of the Field, Prospects for Reform*, eds. Nathaniel Persily and Josh Tucker (New York: Cambridge University Press, 2020), 10-11.

50 Sarah Kreps, “The role of technology in online misinformation,” (Washington, DC: The Brookings Institution, June 2020), https://www.brookings.edu/research/the-role-of-technology-in-online-misinformation; Will Knight, “AI Can Write Disinformation Now—and Dupe Human Readers,” *Wired*, May 24, 2021, https://www.wired.com/story/ai-write-disinformation-dupe-human-readers.

[51] William Galston, “Is seeing still believing? The deepfake challenge to truth in politics,” (Washington, DC: The Brookings Institution, January 8, 2020), https://www.brookings.edu/research/is-seeing-still-believing-the-deepfake-challenge-to-truth-in-politics/.

[52] Christian Vaccari and Andrew Chadwick, “Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News,” *Social Media + Society* 6, no. 1 (January-March 2020): 1-13, https://journals.sagepub.com/doi/full/10.1177/2056305120903408.

[53] Press Trust of India, “Terrorists inciting people via fake news, J&K tells SC,” *The Hindu*, May 1, 2020, https://www.thehindu.com/news/national/other-states/terrorists-inciting-people-via-fake-news-jk-tells-sc-opposes-4g-internet-in-ut/article31479428.ece.

[54] Ashley Deeks, Noam Lubell, and Daragh Murray, “Machine Learning, Artificial Intelligence, and the Use of Force by States,” *Journal of National Security Law & Policy* 10, no. 1 (November 2018): 1-25, https://jnslp.com/2018/11/16/machine-learning-artificial-intelligence-and-the-use-of-force-by-states.

[55] Janosch Delcker, “How Cambridge Analytica used AI,” *Politico*, January 28, 2020, https://www.politico.eu/newsletter/ai-decoded/politico-ai-decoded-how-cambridge-analytica-used-ai-no-google-didnt-call-for-a-ban-on-face-recognition-restricting-ai-exports.

[56] Mark Pomerleau, “An edge for nonstate actors: AI.”

[57] “EU artificial intelligence rules will ban ‘unacceptable’ use,” BBC News, April 21, 2021, https://www.bbc.com/news/technology-56830779.

[58] John Lewis, “The Case for Regulating Fully Autonomous Weapons,” *The Yale Law Journal* 124, no. 4 (January-February 2015): 1309-1325, https://www.yalelawjournal.org/comment/the-case-for-regulating-fully-autonomous-weapons.

[59] Catherine Clifford, “Hundreds of A.I. experts echo Elon Musk, Stephen Hawking in call for a ban on killer robots,” CNBC, November 8, 2017, https://www.cnbc.com/2017/11/08/ai-experts-join-elon-musk-stephen-hawking-call-for-killer-robot-ban.html.

[60] Alexandra Brzozowski, “No progress in UN talks on regulating lethal autonomous weapons,” Euractiv, November 22, 2019, https://www.euractiv.com/section/global-europe/news/no-progress-in-un-talks-on-regulating-lethal-autonomous-weapons.

[61] “PM Modi cautions against weaponization of AI by ‘non-state actors,’” Business Insider, October 6, 2020, https://www.businessinsider.in/tech/news/pm-modi-cautions-against-weaponisation-of-ai-by-non-state-actors/articleshow/78501576.cms.

[62] “Mohsen Fakhrizadeh: ‘Machine-gun with AI’ used to kill Iran scientist,” December 7, 2020, https://www.bbc.com/news/world-middle-east-55214359.

[63] “Artificial intelligence and machine learning in armed conflict: A human-centred approach,” (Geneva: International Committee of the Red Cross, June 6, 2019), https://www.icrc.org/en/document/artificial-intelligence-and-machine-learning-armed-conflict-human-centred-approach.

64 "Appendix D: Draft Legislative Language" in Eric Schmidt, Robert Work, Safra Catz, Steve Chien, Mignon Clyburn, Chris Darby, Kenneth Ford, José-Marie Griffiths, Eric Horvitz, Andrew Jassy, Gilman Louie, William Mark, Jason Matheny, Katharina McFarland, Andrew Moore, "Final Report."

65 Sico van der Meer, "How states could respond to non-state cyber-attackers," (The Hague: The Clingendael Institute, June 2020), https://www.clingendael.org/publication/how-states-could-respond-non-state-cyber-attackers.

66 Patricia Zengerle and David Sherpardson, "US Senate advances sweeping tech bill taking aim at China," Reuters, May 27, 2021, https://www.reuters.com/world/us/sweeping-bill-counter-china-wins-enough-support-advance-us-senate-2021-05-27/.

ABOUT THE AUTHOR

Sarah Kreps is the John L. Wetherill Professor of Government, director of the Tech Policy Lab, and an adjunct professor of law at Cornell University. She is a nonresident senior fellow at the Brookings Institution and the author of five books, including most recently, *Social Media and International Relations* (Cambridge University Press, 2020). Between 1999 and 2003, she served as an active duty officer in the United States Air Force. She has a bachelor's degree from Harvard University, Master of Science degree from the University of Oxford, and doctorate from Georgetown University.

ACKNOWLEDGEMENTS

Lori Merritt edited this paper, Rachel Slattery provided layout, and Richard Li offered helpful research assistance. Chris Meserole offered the generous opportunity to write about the topic of AI and nonstate actors for Brookings.

The Brookings Institution is a nonprofit organization devoted to independent research and policy solutions. Its mission is to conduct high-quality, independent research and, based on that research, to provide innovative, practical recommendations for policymakers and the public. The conclusions and recommendations of any Brookings publication are solely those of its author(s), and do not reflect the views of the Institution, its management, or its other scholars.