ADDRESSING RISKS
FROM NON-STATE ACTORS’ USE
OF COMMERCIALY AVAILABLE TECHNOLOGIES
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALLY AVAILABLE TECHNOLOGIES

DISCLAIMER STATEMENT: The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Companies whose analysts participated in the Public-Private Analytic Exchange Program. This document is provided for educational and informational purposes only and may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and the product of joint public and private sector efforts.
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALLY AVAILABLE TECHNOLOGIES

Executive Summary

Through this 2022 DHS Sponsored Public Private Analytic Exchange Program (AEP), this deliverable addresses risks associated with non-state actors’ acquisition and use of commercially available technologies deemed the most concerning by our research team. The featured technologies were chosen through multiple team brainstorming sessions, presentations by subject matter experts, and independent research. The following content is based on real-world case examples, team members’ professional experiences, and team research. Members of the team endeavored to feature technologies with recent real-world examples affecting the homeland to highlight the likelihood of each technology’s risk of being used by a non-state actor and potential threats in the future as the technologies become more capable and available to non-state actors.

While this deliverable explains how various technologies pose risks to the US government, critical infrastructure, and private sector partners, it does not provide an exhaustive list of all commercially available disruptive technologies used by non-state actors and addresses only those deemed most concerning by this AEP team.

Non-state actors have always been interested in obtaining and utilizing innovative emerging, advanced, or commercially available technologies in support of tactical operations. Non-state actors encompassing terrorist, insurgency, criminal and lone actors are not universally motivated, organized, trained and equipped from one group to the next. The accessibility of commercially available emerging technologies is enabling more globally connected, resourceful, dynamic, well-funded, and technologically savvy non-state actors to level the playing field against better equipped and defended nation states targets. Historically, many emerging or advanced technologies were only available to nation-state militaries, national labs, academic research or industry groups, and a limited number of non-state actors. However, compared to present day, many non-state actors have access across the globe, including those in remote villages, to obtain and use technology such as smartphones. In other cases, new technologies have dramatically expanded threat actor groups’ global reach, with the ability to indoctrinate and recruit instantly via online forums and chat groups and their ability to produce and share propaganda at no cost and with relative anonymity anywhere in the world to distribute it via social media. Non-state actors also use a variety of commercially available platforms for fundraising schemes that have almost no boundaries and exchange of goods and services.

1 Non-state actor refers to criminal, domestic terrorism, or international terrorism threat actors, not at the direction of a specific nation state.
2 Commercially available technology is defined by the U.S. Department of Commerce as a software and/or hardware product that is developed by the technical staff of a government organization for use by the U.S. Government. GOTS software and hardware may be developed by an external entity, with specification from the Government organization to meet a specific Government purpose and can normally be shared among Federal agencies without additional cost. GOTS products and systems are not commercially available to the general public. Sales and distribution of GOTS products and systems are controlled by the Government.
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALLY AVAILABLE TECHNOLOGIES

Additionally, this deliverable touches on non-state actors’ tactical use of these commercially available technologies and tools for conducting hybrid warfare, which is low risk, low cost and provides an adversary the opportunity to obfuscate, throwing doubt on who is responsible for the attack.

Outlook

Several entities across the US intelligence community, private sector security, and critical infrastructure partners all bear the responsibility of protecting US assets against threats from non-state actors in the homeland and abroad. While non-state actors’ use of various commercially available technologies becomes increasingly more mainstream, the US Government is poised to enact policies and regulations to prevent these non-state actors’ from using these certain technologies to attack US interests. Further, if non-state actors continue using these technologies, the US Government and its partners are challenged with creating and using methods to counter non-state actors’ efforts.

---

3 Hybrid warfare entails an interplay or fusion of conventional as well as unconventional instruments of power and tools of subversion. These instruments or tools are blended in a synchronized manner to exploit the vulnerabilities of an antagonist and achieve synergistic effects.
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALY AVAILABLE TECHNOLOGIES

Team Members:

<table>
<thead>
<tr>
<th>Member</th>
<th>Title and Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clare A.</td>
<td>Intelligence Analyst, Amazon</td>
</tr>
<tr>
<td>Deirdre C.</td>
<td>Subject Matter Expert/Senior Manager, Dataminr</td>
</tr>
<tr>
<td>Rachael C.</td>
<td>Lead Security Monitoring and Response Analyst, Fusion Center, Mastercard</td>
</tr>
<tr>
<td>Steve H.</td>
<td>Intelligence Analyst, DC Fusion Center</td>
</tr>
<tr>
<td>Greg M.</td>
<td>Private Sector</td>
</tr>
<tr>
<td>Madeline O.</td>
<td>Global Intelligence Analyst, Royal Caribbean Group</td>
</tr>
<tr>
<td>Stephanie P.</td>
<td>Intelligence Analyst, FBI</td>
</tr>
<tr>
<td>Anissa T.</td>
<td>Intelligence Analyst, NCIS</td>
</tr>
<tr>
<td>Bryce W.</td>
<td>Director of Intelligence Operations, GroupSense</td>
</tr>
<tr>
<td><strong>Team Champion:</strong> Jason L.</td>
<td>Senior Analytic Services (SAS) Officer, NCTC</td>
</tr>
</tbody>
</table>
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALY AVAILABLE TECHNOLOGIES

Technology Summary Table: The following table provides a succinct view of the commercially available technologies listed within this deliverable, a brief description of what each technology is, and highlights of the risks associated by non-state actors’ use of these commercially available technologies.

<table>
<thead>
<tr>
<th>Non-Kinetic (Software Based/Online Technology)</th>
<th>Commercially Available Technology</th>
<th>What is it?</th>
<th>Risks Associated by Non-state Actor Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Platforms</td>
<td>Knowledge Platforms (Google, Quora)</td>
<td>• Social Media and Sharing Platforms (Facebook, Instagram, Twitter, and YouTube)</td>
<td>will further be exploited by terrorists, violent extremists and criminal actors for fundraising, money laundering and exchange of goods and services</td>
</tr>
<tr>
<td></td>
<td>Encrypted Communications Platforms (Telegram, Signal, WhatsApp, Wire)</td>
<td>• Service-Oriented Platforms (cryptocurrency, blockchains, open banking, and person-to-person payment applications)</td>
<td>continued use for hacktivism, terrorist recruitment and propaganda, money laundering, and malign foreign influence</td>
</tr>
<tr>
<td></td>
<td>Digital Platforms</td>
<td>● Machine Learning through algorithms embedded in technology o Digital o Deepfakes o Automated Hacking</td>
<td>will be further exploited by cyber criminals for malign foreign influence operations, hacktivism and fraudulent acts</td>
</tr>
<tr>
<td></td>
<td>Geospatial Intelligence</td>
<td>● Satellite Imagery Including Mobile Applications o Communications/SIGINT o Maxar Technologies</td>
<td>used to create false images or reporting to mislead an adversary, create mis/dis/mal-information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● used by non-state actors to locate goods (drugs) and people in almost real time (law enforcement or military personnel)</td>
<td>used by non-state actors to plan for tactical operations and assist with pre-operational intelligence collection</td>
</tr>
</tbody>
</table>
## ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALCALLY AVAILABLE TECHNOLOGIES

### Technology Summary Table Continued...

<table>
<thead>
<tr>
<th>Kinetic (Hardware Based or Physical) Technology</th>
<th>Commercially Available Technology</th>
<th>What is it?</th>
<th>Risks Associated by Non-state Actor Use</th>
</tr>
</thead>
</table>
| **Unmanned Systems (UxS)**                    | • Unmanned Aircraft Systems (UAS) (Drones, UAV)  
• Unmanned Ground Vehicles (UGV)  
• Unmanned Surface Vessels (USV)  
• Unmanned Underwater Vehicles (UUV) | ● can be used by terrorists for surveillance or to deliver explosive or hazardous payloads  
● criminal organizations have used UAS across state and international lines to smuggle contraband and monitor law enforcement and US military activity | |
| **Additive Manufacturing/3D printing**        | • Privately made firearms (PMFs, aka ‘ghost guns’)  
• Delivery of improvised explosive devices (IEDs)  
• Grenades  
• Counterfeit parts | ● can be used by non-state actors to create untraceable firearms and components for IEDs like an initiation switch or container to conceal an IED inside of | |
| **Tracking Devices**                          | • Mobile phone GPS locator applications  
• Smart watches with GPS tracking features  
• Personal tracking tags (lets users keep track of personal items like their keys, wallet, purse, backpack, luggage, and more through apps) | ● can be used by illicit actors to make their efforts and activities more efficient  
● used by illicit actors to track other citizens in order to establish pattern of life analysis or their belongings (used in criminal stalking cases)  
● used by criminal actors to track drug shipments shipments/deliveries and human trafficking | |
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALLY AVAILABLE TECHNOLOGIES

Key Intelligence Questions

The US intelligence community uses key intelligence questions to address gaps and requirements and guide the collection of information for a given threat. After speaking with technology security professionals representing both the government and the private sector, the team used the following key intelligence questions, which guided the development of the assessment:

1. What novel technologies have the potential to threaten US economic, security, military and space systems?
   a. Who are the non-state actors and what are their efforts to acquire technology that could threaten US interests?
   b. Is the fielding and use of advanced civilian and military technologies that pose a threat to US interests, including directed energy, stealth, counter stealth, materials, computing, AI, unmanned systems telecommunications, nuclear, aerospace and biotech obtainable by nonstate actors and if so what ones are most accessible?
2. How accessible is emerging technology to non-state actors?
3. Why might non-state actors pursue the use of advanced technology, and what would they do with this technology once obtained?
   a. What efforts by state and non-state actors to assimilate and integrate new and advanced technologies are most concerning to the US and its interests?
   b. What are non-state actors’ plans for R&D, or testing, of advanced civilian or dual-use, military technology, or the novel use of old technology?
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALLY AVAILABLE TECHNOLOGIES

Non-kinetic Technology refers to technology that exists in the virtual world, software format or online space. This technology can be used by downloading software to a personal electronic device or computer or by accessing specific websites but is not tangible and not traditionally purchased in a physical setting such as a traditional store.

Digital Platforms are software-based online infrastructure that facilitates interactions and transactions between users. Three main types of digital platforms that non-state actors may exploit are social and media sharing platforms, service-oriented platforms, and knowledge platforms. Within these three types of digital platforms, non-state actors can exploit different functions of each, including harnessing or changing a platform’s AI algorithms to have more favorable outcomes, and using platforms to promote propaganda or spread misinformation, disinformation, or mal-information to sway public opinion or belief. Additionally, non-state actors can utilize these platforms to support their operations by using their communications technologies or for illicit financing. Because many digital and online platforms are now readily available to the public, there are countless types and groups of non-state actors who can utilize these platforms for harmful uses.

1. Knowledge Platforms, such as Google and Quora, are used constantly every day all over the world in a variety of capacities. Knowledge platforms use AI and machine learning frameworks to provide high-quality services to users, such as detecting hostile and destructive content and recognizing spam. Knowledge platforms often have various features and encourage users to create profiles to personalize the user experience. Users with extensive profiles and sensitive information are at risk for malicious actors to conduct cyber-attacks. Non-state actors especially motivated by financial gain are very likely to attack knowledge platforms that contain large
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALLY AVAILABLE TECHNOLOGIES

amounts of data for a variety of reasons like denial of service, ransom or for political or ideological beliefs.

• In 2018, Quora experienced a hack that impacted over 100 million users. Account names, email and IP addresses, user IDs, encrypted passwords, user account settings, and personalization data were among the data compromised in the hack. “Data linked to other networks, such as Facebook, was also accessed, which included “contacts, demographic information, and interests.” Data breaches of knowledge platforms, like the one that occurred to Quora users in 2018, put individuals at risk and could allow for additional attacks on connected networks and platforms.

2. Social & Media Sharing Platforms are online mediums in which members of the public can post and share content, including text, images, videos, and messages, with the intent to broadcast or share it with the public or a subsection or group. Examples of widely used social and media platforms include Facebook, Instagram, Telegram, WhatsApp, Discord, Twitter, and YouTube. Several messaging platforms (Telegram, WhatsApp, Threema) have encrypted capabilities, which enable non-state actors to obfuscate law enforcement and further their malicious intent.

• In July 2022, an Illinois man was charged with seven counts of first-degree murder along with other charges after he allegedly climbed onto the rooftop of a nearby business and opened fire minutes after a July Fourth parade started in Highland Park, Illinois, killing 7 individuals and wounding dozens more. The suspect had years’ worth of disturbing and violent online and social media postings and approximately 5400 followers on Instagram.

• As of July 14, 2022, a federal grand jury indicted a New York man with hate crime violations and firearms offenses in connection with the mass shooting at the Tops grocery store on Jefferson Avenue in Buffalo, New York. On May 14, 2022, 13 people were shot, and 10 died in a racially-motivated attack. The alleged shooter discussed his plans for the attack with users on Discord and 4Chan before livestreaming his attack on Twitch. The livestream was shared in a private Discord group. While fewer than 30 people reportedly saw the livestream, millions of people have seen copies of the footage across digital channels since the attack.

Many non-state actors, including criminals, violent extremists and terrorist groups, use these platforms to post propaganda, recruit members and communicate illicit plans or activities through private or encrypted messaging to obfuscate law enforcement.

• On August 31, 2020, the United States seized “Aletejahtv.com” and “Aletejahtv.org.” The sites acted as Kata’ib Hizballah’s media arm and published internet communications such as videos, articles, and photographs. These communications included numerous articles designed to further Kata’ib Hizballah’s agenda, particularly destabilizing Iraq and recruiting others to join their cause. They also functioned as a live online television broadcast channel,
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALLY AVAILABLE TECHNOLOGIES

“Al-etejah TV.” Portions of the communications expressly noted that they were published by Kata’ib Hizballah.\textsuperscript{xii}

Social and media sharing platforms have algorithms that use deep learning technology to best serve users. Many social media applications, such as Twitter, use algorithms that rely heavily on user bias to propagate content to Twitter users.\textsuperscript{xiii} Twitter’s algorithm uses a predictive model that shows content with high numbers of interactions to more users. This allows “popular” or trending content to be shown to more users and can cause content to go “viral.” These functions can also aid non-state actors in anonymously spreading disinformation or misinformation to a wide audience in order to solicit increased support or motivate violent actions on behalf of the non-state actor groups. The use of social and media sharing platforms in this manner enables globally dispersed external operations by recruiting, eliciting and engaging ideological affiliated followers from different locations around the globe.

- In 2020, the United States located the content from “Aletejahtv.com” and “Aletejahtv.org” on “Aletejahtv.com” and “kataibhezbollah.com,” including the Kata’ib Hizballah flag and the words “Islamic Resistance, Kataib Hizbollah.” The content even included false information about COVID-19 designed to damage the perception of the United States in the minds of Iraqi citizens and to destabilize the region to the benefit of Iran.\textsuperscript{xiv}

Using these platforms to promote disinformation may be the most concerning given the variety of uses by non-state actors with the intent to disrupt, cause confusion, misconstrue or manipulate opinions. Several types of disinformation campaigns include foreign influence, political disinformation, issue-based disinformation, and lucrative disinformation, as described by Graphika’s Chief Innovation Officer in 2020.\textsuperscript{xv} Foreign influence disinformation is carried out by foreign states and occasionally by their proxies and is the use of disinformation to disrupt societies or certain issues to push an agenda. Political disinformation can also be carried out by state actors and is the use of disinformation to undermine adversaries or push political agendas; however, domestic politicians and political parties can also use fake identities to sway public opinion about another political party or have also been known to spread political disinformation. Issue-based disinformation is the use of disinformation to serve an ideological, normative, and/or financial goal, and lucrative disinformation is the use of disinformation to make a profit; these two are the most likely to be used by non-state actors. By creating fake identities and profiles and sometimes harnessing bots or AI technology to help spread their message, a slew of actors can spread issue-based disinformation online, including activists, religious bodies, consultancies, extreme supporters, NGOs, and many other groups. Non-state actors who spread disinformation for monetary gain can include PR firms, fringe networks, or even just average social media users. Most frequently, these actors will set up a clickbait to drive social media traffic to fake websites and gain monetary value from advertising. They can also design financial scams, which frequently include sensational topics to attract attention.
On 27 January 2021, US officials arrested a Florida resident for “conspiring with others in advance of the 2016 US Presidential Election to use various social media platforms to disseminate misinformation designed to deprive individuals of their constitutional right to vote.” The individual conspired with others to exploit social media platforms, including Twitter, to send fake messages telling individuals that they could “vote” via text message or on social media, rather than using legal methods of voting.

AI and machine learning systems can be used to initiate cyber-attacks through digital platforms that could impact any smartphone user. Likewise, this also presents the opportunity for any smartphone user to be a potential malicious actor. Social and media sharing platforms use different AI systems to run applications and best serve users. However, these systems can be weaponized to cause damage to companies or target individuals.

Some features of social media platforms have been weaponized by non-state actors to cause reputational damage to companies. While instances of weaponized AI mostly have virtual impacts, damages to reputation and credibility can cause financial loss and have secondary effects that could include physical impact. In 2016, Microsoft developed a chatbot named “Tay” to “conduct research on conversational understanding” among 18–24-year-olds. Twitter users manipulated Tay’s algorithm until the chatbot tweeted racist comments and cited Adolf Hitler. Microsoft issued an extensive public apology and had to detect and patch the chatbot’s vulnerability that non-state actors exploited and improve the security of the algorithm.

3. **Service-Oriented Platforms:** As cryptocurrency, blockchains, open banking, and person-to-person payment applications usage rates increase, non-state actors will look to exploit the popularity and novelty of these digital platforms and assets. Beyond the risks of fledgling security measures and business practices of the multiple new players in the market, regulatory policies lag behind this innovative technology; further, the general public’s comprehensive understanding of new technology and awareness of its associated risks also struggle to keep pace. While any novice familiar with the financial industry and even remotely savvy with the internet can find a slew of instructions on how to fraudulently fund their illicit activities in a matter of minutes, non-state actors are known to be early adopters of technology, making their sophisticated use of it even more perilous.

While consumers remain cautious in adopting cryptocurrency use in their daily activities, criminals are well versed in the benefits of the blockchain. Its low transaction costs increase profit, while its decentralized finance (DeFi) protocols allow for quick swapping between different types of crypto to further anonymize their earnings and avoid law enforcement attention. According to a 2022 report by blockchain data company Chainalysis, “criminals laundered $8.6bn of cryptocurrency in 2021, up by 30% from the previous year.” These criminals include drug traffickers, ransomware attackers, malware operators, scammers, human traffickers, dark net market operators, and terrorist groups.
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALLY AVAILABLE TECHNOLOGIES

- In February and March 2022, various extremist groups began advertising new cryptocurrency and money transfer options on their websites for international donors amid Russia’s invasion of Ukraine.\textsuperscript{xxi,xxii}

- In February 2022, the DOJ arrested a husband and wife duo for allegedly conspiring to launder 119,754 BTC stolen during the 2016 hack of the Bitfinex cryptocurrency trading platform. Additionally, the DOJ seized $3.6 billion in cryptocurrency linked to the stolen funds.\textsuperscript{xxiii}

- In August 2020, the DOJ dismantled three terrorist financing cyber-enabled campaigns involving HAMAS, al-Qa’ida, and a noncompliant cryptocurrency exchanger, seizing more than 300 cryptocurrency accounts. This marked the largest seizure of public cryptocurrency assets tied to terror finance in CT history. According to the same DOJ complaint, Syrian-based al-Qa’ida facilitators operated as a bitcoin money-laundering network, posing as charitable institutions, and using Telegram channels to raise money for weapons and supplies.\textsuperscript{xxiv}

- In March 2020, a dual US citizen was sentenced to 13 years in prison in New York for providing material support to ISIS through money laundering involving cryptocurrency. Over the course of multiple months in 2017, the offender attempted to send funds to ISIS involving bitcoin derived from credit-card fraud.\textsuperscript{xxv,xxvi,xxvii}

With the introduction of real-time payments online, via smartphones or self-service machines, and as consumers increasingly conduct more transactions digitally, authorized push payment fraud losses increase. Criminals lure victims into sending money using stolen or invented identities and fake websites, emails, and phone calls to circumvent banks’ stringent security checks. Unlike the consumer protection of PCI DSS and card brand rules (Regulation E, dispute lifecycle, liability), these are irrevocable payments.
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIAL AVAILABLE TECHNOLOGIES

Artificial Intelligence (AI)

AI capabilities have grown at an unprecedented rate, and these technologies have many widely beneficial applications. Advances in AI have made it easier to acquire the technology for both its constructive and illicit uses. Low-cost, commercial off-the-shelf AI means that a range of non-state actors can increasingly adopt these technologies in the digital and physical security realms.

AI refers to “the ability of a machine to learn from experience, adjust to new inputs and perform human-like tasks.” 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.xxviii

Digital: In the digital domain, AI is enhancing cyber capabilities that could be weaponized by non-state actors. Politically motivated terrorist groups use cyber to effect political change by intimidating other audiences and recruiting and radicalizing like-minded individuals through propaganda. Cybercriminals also use this domain to exploit online user data for financial gain. Non-state actors have employed spear phishing to steal data and then sell it; other times, they use ransomware to hold a victim’s information and then ask the individual for ransom payments to regain access.xxx

- In 2021 and 2022, DOJ sentenced members of the international hacking group FIN7 for breaching corporate computer networks across the United States. FIN7 stole more than 20 million customers’ PCI from individual point-of-sale terminals across thousands of business locations.xxx

Machine learning is a subset of AI and is used to teach machines/systems to make predictions and acquire and develop knowledge. Machine learning behaviors enable systems in AI to be automated to support everyday tools such as online platforms and mobile applications.

AI can enhance non-state actor cybercrimes in numerous ways, and hackers continue to develop new tools and techniques to sophisticate the cyber-attack process. One prolific example of
enhanced cybercrime has been the improved efficiency of phishing schemes. Non-state actors can leverage natural language processing methods to improve existing phishing email content. AI can be used to create emails to bypass enhanced security technology, allowing financially motivated non-state actor groups to further spread malware necessary for their ransomware and other cyber operations.xxxi

- On May 7, 2021, the US Colonial Pipeline – which supplies about 45 percent of the East Coast’s fuel – was the victim of a ransomware attack. The ransomware variant that impacted Colonial Pipeline’s network is DarkSide, a Ransomware-as-a-Service (RaaS) in which the developers sell hackers access to their malware. This incident serves as a stark reminder of the significant impacts of a ransomware infection in a critical infrastructure environment, even without impacting OT systems. Colonial Pipeline lost substantial revenue due to the extended period that their operations were shut down, and, as speculation circulated, the pipeline’s servicing population was concerned that fuel would not be available to purchase, which temporarily drove up gas prices and the availability of fuel for consumers.xxxii xxxiii

**Deepfakes** are a type of AI that use generative adversarial networks (GANs), a machine learning system that follows a constant-learning type of behavior. Deepfakes are widely accessible - there are apps available for smartphone users to easily create their own deepfakes. Deepfakes can be used by non-state actors to exploit individuals by creating falsified photos or videos to incriminate victims, demand ransoms and spread disinformation.xxxiv

Deepfakes can also be used to mimic voices. Non-state actors have used audio deepfakes to carry out virtual kidnappings, wherein a victim is called over the phone and malicious actors make false claims that they have taken a relative of the victim hostage and play falsified pleas for help from the victim’s relative. Malicious actors demand money transfers in return for the release of hostages.xxxv

- In April 2022, the United States announced the seizure of the RaidForums website, a popular marketplace for cybercriminals to buy and sell hacked data, and unsealed criminal charges against RaidForums’ founder and chief administrator, Diogo Santos Coelho, 21, of Portugal. Beginning in 2015 through February 2022, RaidForums served as a major online marketplace for individuals to buy and sell hacked or stolen databases containing the sensitive personal and financial information of victims in the United States and elsewhere, including stolen bank routing and account numbers, credit card information, login credentials and social security numbers. RaidForums members used the platform to sell hundreds of databases of stolen data containing more than 10 billion unique records for individuals residing in the United States and internationally. At the time of its founding in 2015, RaidForums also operated as an online venue for organizing and supporting forms of electronic harassment, including by “raiding” – posting or sending an overwhelming volume of contact to a victim’s online communications medium – or “swatting” – the practice of
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALLY AVAILABLE TECHNOLOGIES

making false reports to public safety agencies of situations that would necessitate a significant, and immediate armed law enforcement response.xxxvi

- In 2019, a threat actor used AI-enabled voice deepfake technology to convince the CEO of a UK-based energy firm to transfer nearly $250,000 to a bank account controlled by the threat actor. The CEO mistakenly thought he was speaking to the CEO of his parent company because the deepfake voice matched his boss’ voice.xxxvii

Automated Hacking: Sophisticated methods in AI have been developed by malicious non-state actors to detect and exploit vulnerabilities quickly in organizations and agencies. AI and machine learning systems can automate hostile cyber-attacks and increase the impact of attacks. Automated hacking allows for adversaries to quickly and efficiently plan, initiate, and execute cyber-attacks while minimizing repetitive or tedious work in the cyber-attack process.xxxviii

Search engines such as Shodan and Censys can scan the internet and collect information for billions of IP addresses around the world.xxxix Malicious actors can use these services to find targets of attacks quickly. For instance, “if a new exploit is found in...Microsoft Exchange Server, [hackers] can just enter a query on Shodan to find all servers connected to the internet that are running that version of Exchange and get a list of IP addresses that they can then use to launch their attacks.”xli

Online tools, such as AutoSploit, can automate the hacking process by taking the data provided by search engines like Shodan and Censys. Integrated attack frameworks like AutoSploit allow hackers to easily “run a search, launch an attack, and receive a list of exploited servers.”xlii

AI and machine learning systems are constantly being developed and improved by malicious non-state actors to increase the impact of attacks. Sophisticated tools and systems are often used to target businesses and agencies that could be financially exploited or contain massive data collections. However, the prolific daily use of smartphones and knowledge platforms by individuals presents many security vulnerabilities.
The proliferation of geospatial intelligence (GEOINT), specifically commercially available satellite imagery, has the potential to threaten US interests through their use by non-state actors to track the movements of security forces, enhance terrorist attack plotting, and spread mis/dis/mal-information either intentionally or accidentally through the spread of unvetted analysis. The ability of potential attackers to exploit publicly available geospatial information significantly varies with the type of information needed.xlii

**Terrorists:** Commercially available imagery potentially allows non-state actors to collect detailed information on facilities and security measures, enhancing attack planning. This can be particularly true when combined with other open sources such as news reports and social media postings.

- In 2018, an FTO-inspired attack planner used mapping software to identify the best place to detonate explosives during an Independence Day celebration, plotting the locations of fireworks launches, federal buildings, and crowds of attendees.xliii
- In 2022, a New York resident was convicted of providing support to an FTO by providing maps of battlefield conditions that may have enabled lethal attacks in a foreign country.xliv

**Mis/dis/mal-information:** The proliferation of imagery in open source settings creates the potential for information to be misinterpreted or misused, whether intentionally or inadvertently. Risks include revealing facts that might precipitate a crisis or make responding to one more difficult.xlv The misinformation could be the result of errors in interpretation or from false geospatial data inserted into a data stream by a malicious actor in a process labeled “location spoofing” by researchers.xlvi

- In 2011, a group of students at a US-based university published research claiming to have located storage for thousands of previously-unknown Chinese nuclear weapons, based partly on commercial imagery of a supposed tunnel system. Though experts debunked the
findings as infeasible technologically based on known amounts of plutonium in Chinese weapons, major news organizations reported the study as fact\textsuperscript{xlvii}

High-quality satellite imagery used to be available only to governments. Since the early 2000s, advances in technology combined with the loosening of regulations in the United States and increasing foreign competition made the same type of imagery commercially available. A key moment in the process came in 2007 with the launch of two European satellite arrays, which made Synthetic Aperture Radar (SAR) images down to the range of less than one meter available to the civilian market.\textsuperscript{xlviii} Since then, the market has dramatically expanded, with hundreds of satellites now available with the capabilities of seeing through weather and foliage at high resolution.\textsuperscript{xlix}

Perhaps the simplest GEOINT technology – Google Earth – is available to anyone with an internet connection. Images of a higher resolution or more frequently monitored areas are available for a cost. While some of these services require an individual to contract with a provider, many of whom primarily service governments, others are offered at a nominal cost. For example, a Slack channel in which users crowdsource various GEOINT projects can be accessed for $5 a month.\textsuperscript{l}

As the market for commercial satellite imagery developed, foreign governments loosened regulations and promoted their domestic industries, leading to Chinese and European companies gaining market share and eroding American technological leadership in the field. While this has led some commentators to promote an “industrial policy” to promote American commercial imagery\textsuperscript{li} any such actions would have to engage with the trade-offs inherent in promoting industry while mitigating the security vulnerabilities inherent in the technology.
Kinetic Technology refers to those technologies that produce a physical effect on a targeted area, physical technological devices or equipment used in a tangible manner or to produce a tangible product. For example, a bullet impacting a target is a kinetic engagement. The following three categories, UAS, additive manufacturing, and tracking devices, are considered hardware-based technology that are also commercially available and used by non-state actors.

Unmanned aircraft systems (UAS), or “drones” have the is a demonstrated threat to US interests through their deployment by non-state actors in operations against US interests both abroad and domestically, criminal usage including smuggling, surveillance or disruption of critical infrastructure, and their potential usage in terrorist attacks.

UAS are part of a broader scope of unmanned systems (UxS), which includes ground, surface, underwater, and aerial vehicles. Commercially-available UxS are a low barrier-to-entry tool allowing non-state actors to conduct reconnaissance and surveillance, attacks, and coordinate criminal activity with greater flexibility. As this analysis is concerned with non-state actors’ use of commercially-available technologies, the primary focus in this deliverable is UAS, which are utilized by the studied actors at a much higher rate in comparison to unmanned ground and underwater systems. At present, the majority of substantive, malicious UAS activity occurs outside the United States, primarily in the Middle East with growing activity in Latin America. The primary risk presented to the US security and stability exists outside US borders, by attacks targeting US and partner nation institutions. However, a range of malicious actors in the US and along its borders have expressed interest in incorporating these technologies to further their goals in the US and traditionally-secure locations.

UAS are not “novel” compared to some of the technologies examined in this report. There have been unmanned aircraft on battlefields for almost as long as there have been manned aircraft. The first known terrorist plot to use a UAS (in the form of a model airplane) was a foiled assassination attempt by the Red Army Faction in Germany in 1977. As far back as the mid-

---

[Page 19]
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALLY AVAILABLE TECHNOLOGIES

1990s, the US Government was considering planning scenarios involving terrorists using UAS to disperse biological weapons, similar to an abandoned plot by Japanese cult Aum Shinrikyo around the same time.\textsuperscript{1990s}

Still, as UAS technology evolves, threat actors will likely use UAS in novel ways which may challenge existing security measures. While non-state use and seek UAS on the battlefield, their use in violent attacks in the homeland has so far been limited. Only a small portion of the lethal use of UAS technology has been exploited by non-state actors, making this specific type of unmanned systems technology well-suited as a case study to help us to understand the risks associated with these emerging technologies.

**Insurgents:** The most notable and sustained threats to US interests from non-state actor use of UAS comes from insurgent groups who have or may engage the US military and interests abroad. ISIS made prolific use of commercially available UAS technology to surveil, guide operations, and conduct weaponized attacks with droppable explosive devices on targeted areas within Iraq and Syria. Before its territorial losses in Iraq and Syria, the organization’s UAS program hindered efforts by American and allied forces to retake territory and provide support to fleeing civilian populations. Other designated Foreign Terrorist Organizations (FTOS), including Hizballah, HAMAS, and Houthi militias, have advanced UAS programs, though they have to date used them primarily in conventional conflicts against states.

**Terrorist Attackers in the Homeland:** While numerous commentators have warned of the potential for terrorists to use UAS in attacks against the homeland, none have been known to have succeeded. Supporters of FTOs have expressed intent to use UAS in the homeland, but plots have been disrupted at the planning stages:

**Domestic extremists** have thus far expressed little interest in UAS attacks, according to academic sources.\textsuperscript{4} However, this does not preclude the possibility of a lone actor deciding to use a UAS in the future. An attacker could use a UAS for surveillance of a target long before law enforcement is aware of the nefarious nature of a flight:

- In February 2019, Wesley Dallas Ayers of Anderson, South Carolina, was sentenced in federal court to 361 months in federal prison and five years of supervised release. Ayers constructed and then placed three explosive devices in various parts of Anderson County between January 24, 2018, and February 24, 2018. Ayers used a drone to deliver at least one explosive device. A device placed by Ayers on January 30, 2018, at the intersection of Travis and Martin Roads in Anderson County, detonated and injured one individual. The other two devices, which Ayers also placed in or near area roadways, were intercepted and rendered safe by federal, state, and local law enforcement agencies. In that same timeframe, Ayers placed three hoax devices, which resembled explosives but did not contain any blasting agent. With some of those devices, the defendant left threatening messages that more, and more powerful, devices were to come.\textsuperscript{5,6}
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALLY AVAILABLE TECHNOLOGIES

Unaffiliated Lone Actors: Individuals without a known terrorist nexus have demonstrated the ability to use UAS for malicious purposes, though such incidents remain limited:

- In December 2019, a Pennsylvania man pled guilty to using a UAS to harass a former girlfriend, reportedly modifying his UAS to drop small explosives on her property.\(^{lviii}\)

Transnational Criminal Organizations (TCOs): Many criminal actors have integrated UAS into their operations. Perhaps the most concerning are TCOs, including Mexican drug cartels. These cartels are often similarly resourced to larger FTOs and use UAS for similar purposes – including both in surveillance and attacks on law enforcement or rival criminal organizations. Certain organizations in Mexico have modified UAS to drop small explosives at least since 2017.\(^{lix}\) While TCO lethal attacks using UAS remain in inter-group conflict outside the United States, Mexican drug trafficking organizations (DTOs) are increasingly using UAS to surveil smuggling routes and transport small amounts of narcotics along and across the US-Mexican border – perhaps as many as several thousand incursions a year, according to one advocacy organization.\(^{lx}\)

<table>
<thead>
<tr>
<th>UAS Groups</th>
<th>Maximum Weight (lbs) (MGTOW)</th>
<th>Normal Operating Altitude (ft)</th>
<th>Speed (kts)</th>
<th>Representative UAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group 1</td>
<td>0 – 20</td>
<td>&lt;1200 AGL</td>
<td>100</td>
<td>Raven (RQ-11), WASP</td>
</tr>
<tr>
<td>Group 2</td>
<td>21 – 55</td>
<td>&lt;3500 AGL</td>
<td>&lt; 250</td>
<td>ScanEagle</td>
</tr>
<tr>
<td>Group 3</td>
<td>&lt; 1320</td>
<td>&lt; FL 180</td>
<td></td>
<td>Shadow (RQ-7B), Tier II / STUAS</td>
</tr>
<tr>
<td>Group 4</td>
<td>&gt;1320</td>
<td>&gt; FL 180</td>
<td>Any Airspeed</td>
<td>Fire Scout (MQ-8B, RQ-8B), Predator (MQ-1A/B), Sky Warner ERMP (MQ-1C)</td>
</tr>
<tr>
<td>Group 5</td>
<td></td>
<td></td>
<td></td>
<td>Reaper (MQ-9A), Global Hawk (RQ-4), BAMS (RQ-4N)</td>
</tr>
</tbody>
</table>

The Department of Defense classifies UAS into five groups based on size, speed, and operating altitude.\(^{lx}\)

The highest groups (4 and 5) are almost certainly out of the range of acquisition for all but state actors in the near future. Group 3 UAS are predominately state-manufactured; however, Hizballah, Houthi, and HAMAS operate UAS, which are likely in Group 3. These organizations are outliers in that they are well-resourced and benefit from high levels of state support. UAS meeting the criteria for Groups 1 and 2 are most likely available to any actor with access to a hobby store or reliable delivery service.
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALY AVAILABLE TECHNOLOGIES

With commercial UAS systems widely accessible, the primary barrier to further lethal use is successful weaponization of the system and investment by non-state actors in their development and implementation when other considerably cheaper and easier to use attack scenarios are available. Research on ISIS and HAMAS UAS programs suggests the importance of skilled personnel and at least some sort of dedicated program to weaponize UAS effectively. Barriers to entry have likely fallen in the previous few years as technology advanced, and non-state actors have benefited from advances among do-it-yourself hobbyists and other information shared from non-state actors online.

The Cybersecurity and Infrastructure Security Agency (CISA) notes four risks from illicit UAS:

1. **Weaponized or Smuggling Payloads** – Depending on power and payload size, UAS may be capable of transporting contraband, chemical, or other explosive/weaponized payloads.
2. **Prohibited Surveillance and Reconnaissance** – UAS are capable of silently monitoring a large area from the sky for nefarious purposes.
3. **Intellectual Property Theft** – UAS can be used to perform cyber-crimes involving the theft of trade secrets, technologies, or sensitive information.
4. **Intentional Disruption or Harassment** - UAS may be used to disrupt or invade the privacy of other individuals.

The most concerning of the four is weaponization and smuggling, as those two would have the greatest kinetic impact on lives and property in the US.

A Department of Defense-funded study suggested that novel threats pursuing weaponized attack techniques, including UAS, could be modeled along two pathways: either the actor chooses the target and finds a UAS to be uniquely useful for attacking that target or the adversary wishes to use a UAS then finds a suitable target. In the first pathway, the adversary finds that a UAS solves a problem that a conventional weapon may not. This can help explain why UAS have proliferated on the battlefield where non-state actors are outmatched by state competitors in the air. It also describes those actors who use UAS to conduct surveillance that would be risky or impossible to do in other ways. The second pathway may describe those actors with a special skill in UAS technology or those who might insist on using a UAS for their own reasons. The subject who plotted the UAS attack on the Pentagon, for example, told undercover officers that a conventional attack with a rifle would not satisfy him as he wanted to “go big.”

There is little information available in open sources regarding future plots by non-state actors to weaponize or otherwise employ UAS.

**Artificial Intelligence (AI)** will create new opportunities and make capabilities more affordable to various organizations, including non-state actors. Lethal autonomous technology combined with commercially available AI could enhance non-state actors’ lethality while minimizing exposure and reducing the need for human capital, intelligence, and expertise to accomplish specific tasks. Specifically, AI used for military programs and the repurposing of commercially available AI
technology can potentially improve non-state actors’ lethality. The innovation of AI and machine learning has made it possible to automate systems in defense technology. Automated weapons systems are driving offensive and defensive military operations around the globe. Unmanned naval, aerial, and terrain vehicles use AI for navigation and utilization. “Fire and forget” missile systems are deployed using AI and radar systems that allow it to lock onto targets and execute attacks.

While automated weapons are mostly used by state actors, there is a growing demand from non-state actors to possess these types of weapons. Non-state actors could also attempt to hack the AI software of automated weapons, which could have detrimental impacts. If an automated weapon were to attack the wrong target after being hacked or cause civilian casualties, large-scale conflicts could develop and threaten global security.
A second example of hardware-based kinetic technology utilized by non-state actors is additive manufacturing (AM) technology, also commonly known as 3D printing, which presents additional risks for the homeland. Possessing and using a 3D printer is legal and is not indicative of illicit activity; however, non-state actors may use AM to print privately made firearms (ghost guns), or at least parts to a whole, items that support the manufacturing of components that can be used in the production of IEDs, UAS airframes or replacement components and other unique items that can support non-state actors illicit activities. AM is the process of creating a 3D solid object from a digital model through layered addition of materials. AM can be used for rapid prototyping, in situ production and repair of deployed military equipment, and production of precision, custom or unique parts. Although AM technology has many legitimate applications, including easily replicating small items like paper clips, coat hangers and broken refrigerator door handles, it can enable non-state actors to evade law enforcement by reducing their identifiable actions during the acquisition phase of components needed to support their tactical operations and may lower the cost of production for various types of dangerous weapons used to carry out attacks.

Commercially Available and Becoming Cost Effective: AM is becoming increasingly popular, and its capabilities with design complexity and control are becoming more advanced, allowing for more involved detailed 3D prints to be achieved by users. 3D printers are becoming cheaper (basic models can be bought online for as little as $180) and commercially available (can be found in basic computer stores and online stores) but are typically restrained to print plastic objects. Other 3D printers allow for a variety of material capabilities and can use metals, ceramic, and carbon fiber, with glass as a possibility but are more complicated to achieve and expensive to acquire. Some printers melt ceramic products to achieve desired products. More recently, companies have been looking to lower the cost of metal 3D printing to make it more accessible. Further appeal of 3D printers include ease of acquiring schematics (schematics are being shared on open source websites for free); however, one does not have to rely solely on using the computer-aided design (CAD) software. Further convenience and accessibility come from 3D print centers where an
individual can go and upload their files for mass production of items, sometimes using higher grade 3D printers with better materials.

**Explosives:** Additional benefits of using a 3D printer include printing conductive filaments, which aid in making explosives. Further, hobbyists can easily turn to publicly available online stores for multiple free AM technologies. Currently, academia is exploring even more desirable capabilities, such as enabling 3D printers to stop or retrace and correct their mistakes, which allows for more flawless products and printing complex objects like UAS or drones from start to finish, including internal mechanics.\textsuperscript{ixii}

**UAS:** In 2014 and again in 2020, students from the University of Virginia and Virginia Tech worked together using 3D printing technology to produce a UAS airframe using a remote control with navigation (mobile phone), allowing it to fly without an expensive navigation system and shared lessons learned.\textsuperscript{ixiii,ixiv,ixv}

**Labware:** AM appeals to non-state actors for the aforementioned reasons as well as a perceived obfuscation. An object created, or part of a whole object created, with a 3D printer may not be easily traceable and can make it easier for nefarious actors to obfuscate law enforcement. Non-state actors can use 3D printers to make IED components or devices, labware (micro-pipets, flasks) or reactionware (custom-built laboratory containers for chemical synthesis). Given some labware (i.e., for illegal drug manufacturing) is illegal to own or buy, the ability to manufacture these items with a 3D printer enables the illegal drug makers to build a lab with equipment that is illegal for them to obtain through traditional legal channels.\textsuperscript{ixvi}

**Privately Made Firearms:** Non-state actors, primarily lone-actors, can and are using 3D printers to manufacture firearms components. Technological developments have allowed for the 3D printing of firearms and firearm parts, including parts made out of plastic, by unlicensed individuals in possession of relatively inexpensive 3D printers.\textsuperscript{ixvii} From January 2016 to December 2021, ATF received approximately 45,240 reports of suspected privately made firearms recovered by law enforcement, including in 692 homicide or attempted homicide investigations. The Department of Justice is actively seeking to limit these untraceable privately made firearms by submitting to the Federal Register the “Frame or Receiver” Final Rule, which modernizes the definition of a firearm and will help close the loophole related to selling frame and receiver kits for privately made firearms. Once implemented, this rule will clarify that parts kits that are readily convertible to firearms are subject to the same regulations as traditional firearms. These regulatory updates will help curb the proliferation of privately made firearms, which
are often assembled from kits, do not contain serial numbers, and are sold without background checks, making them difficult to trace and easy to acquire by criminals.\textsuperscript{lxxviii}

Individuals wanting to purchase a gun but fail a background check can instead use a privately made firearm, for example, a firearm made from an unfinished AR-15-style receiver to carry out heinous acts of violence. STL files, computer files used for 3D printing items, for an unfinished firearm frame or receiver that can be built into a functional firearm, and 3D-printed guns or guns made with 3D-printed receivers have been recovered by law enforcement as travelers attempted to transport the firearms through checkpoints. Firearms 3D-printed in plastic may be able to evade detection by metal detectors at security checkpoints, increasing the risk that a firearm may be used to perpetrate violence on an airplane or other congested areas. The availability of online code for the 3D printing of firearms and firearm parts increases the risk that dangerous people, including felons, domestic abusers, and other people prohibited from possessing firearms under federal law, as well as terrorists and criminals around the world, will evade background check requirements and obtain a firearm through 3D printing.\textsuperscript{lxxix}

4D printing is the process through which a 3D printed object transforms itself into another structure over the influence of external energy input as temperature, light or other environmental stimuli over time. The advantage of 4D printing over 3D printing technology is its ability to change shape over time. A 4D printed object is printed just like any 3D printed shape. The difference is that the 4D printing technology uses programmable and advanced materials that perform a different functionality by adding hot water, light or heat. 4D printing technology uses commercial 3D printers and then a “smart material” that can be either a hydrogel or a shape memory polymer. Their thermomechanical properties and other material properties give smart material the attributes of shape change and are differentiated from the common 3D printing materials.\textsuperscript{bxx}

One potential application of 4D printing in the real world would be pipes of a plumbing system that dynamically change their diameter in response to the flow rate and water demander; they may heal themselves automatically if they crack or break. Since 3D printing is limited by the size of the

Privately Made Firearms – Member of “Boogaloo Bois” Pleads Guilty to Conspiracy to Provide Material Support to Hamas

On 4 May 2021, a Minnesota man and member of the “Boogaloo Bois” pleaded guilty to one count of conspiracy to provide material support to a designated FTO. The defendant and confidential human source (CHS) met an undercover employee of the FBI (UCE) that the defendant believed was a member of Hamas. During this meeting, the Boogaloo Bois members proposed manufacturing suppressors, untraceable firearms and fully automatic firearms for Hamas. At a later meeting, the defendants gave the UCE a 3D printed “auto sear” believing that the auto sear would be used by Hamas to convert semi-automatic rifles into fully automatic rifles. The defendants then agreed to obtain, and did obtain, another order of auto sears for the CHS and the UCE.

Source: Department of Justice | Office of Public Affairs Press Release | “Second Member Of ‘Boogaloo Bois’ Pleads Guilty to Conspiracy to Provide Material Support to Hamas” | https://www.justice.gov/opa/pr/second-
printer, 4D printing may enable the capability to print furniture by printing a flat item that would
morph into a chair when exposed to an external stimulus such as water or light.\textsuperscript{xlii}

Objects printed with 3D printing technology are characterized by rigidity, and these 3D printed objects are going to keep their 3D shape once printed. Therefore, the adaptability of 4D printing would be useful in large-scale projects and in extreme environments, such as space to build bridges or shelters, as they would build up themselves or repair themselves in case of weather damage. Additionally, 4D printing can be applied to small-scale projects and in sectors such as the medical field. Some additional materials researchers are working on include self-folding protein and medical stents. Programmed stents would travel through the human body, and opening up when they reached their destination.\textsuperscript{xxxii} And for infrastructure-related projects, 4D printing could design pipes to adapt, expand, or contract based on their surroundings. Similarly, this adaptability could permit a range of innovative capacities such as “self-healing” pipes and equipment to counteract cracks or wear as well as “self-disassembling” materials to facilitate recyclability.\textsuperscript{xxxiii}

As 4D printing is adopted by mainstream manufacturing, the underlying security remains unstable and susceptible to exploitation by non-state actors. Using 4D printing in critical applications, such as aircraft and medical devices, could open the door for malicious attackers to cause deadly or catastrophic product failures. A hacker who gains access to a computer or the printer that uses additive manufacturing could manipulate designs to fail at specific times during the external influence phase of the item over time. Therefore, the best defense is quality control with stringent testing and scans prior to public release.\textsuperscript{xxxiv}

Technological advances in AM will continue to allow these devices to become more widely used, accessible and commercially available. With progress comes risk, however, and the homeland faces constant threat from non-state actors continuously looking for ways to obfuscate law enforcement and incorporate the latest technology into their techniques, tactics and procedures. AM technology may provide non-state actors with the ability to create dangerous, homemade, and difficult to trace weapons or tools ultimately either to execute a drug operation, give support to terrorist organizations, hack and harm critical infrastructure facilities, or conduct a terrorist attack.\textsuperscript{xxxv}
Commercial tracking devices prove to be another example of kinetic technology used by non-state actors, and have the potential to threaten US interests and may be used by criminals, DTOs, or individuals for targeted violence.

Tracking devices analyzed for this report consist of small, Bluetooth-enabled devices which can be attached to items (backpacks, vehicles, keychains) and remotely connected to smartphones or tablets. These devices are commonly used to keep track of items that might be valuable or easily misplaced, such as car keys.

Evidence for nefarious use thus far has been limited, in contrast with some of the other technologies this report considers. While this makes analysis more difficult due to the lack of systemic data collection efforts or existing academic analyses, Bluetooth trackers an ideal test case for the models and theories developed in the report as an emerging technology with the potential to become more prominently used in the future.

**Criminal Actors:** Since 2021, there have been numerous reports of tracking devices allegedly used in a variety of criminal activities especially stalking and targeting vehicles for theft. Information on these activities has mostly come in the form of news reports on local crime and public safety messages from local law enforcement agencies.\textsuperscript{xvi}

**Drug Traffickers:** DTOs have long been innovative in their methods of evading detection while shipping drugs across international borders. Some Latin American organized crime groups have long used Global Positioning System (GPS) technology to monitor the status of shipments.\textsuperscript{xvii}
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALY AVAILABLE TECHNOLOGIES

- In 2015, the leader of the Sinaloa Cartel escaped from prison using a GPS tracker in a watch.\textsuperscript{lxxxviii}

It is reasonable to assume that tracking devices could deliver similar capabilities at a lower cost. While Bluetooth tracking devices have been on the market for several years, they have exploded in popularity since 2021 with the introduction of Apple’s AirTags brand, which made the technology more affordable and accessible compared to previous generations of such commercial GPS devices. In addition, AirTags improved upon the location accuracy of previous models.\textsuperscript{lxxxix}

The reported widespread use of newer tracking devices meets many of the criteria for technology adoption advanced by a university professor in work on innovation in terrorist groups. The author theorizes that the technologies likely to be adopted for malicious use share twelve criteria. Notably, these include accessibility, effectiveness, and “not cutting-edge” (within a second or third generation of commercial development).\textsuperscript{xc} These newer models are likely to be attractive as they are a second-generation technology and more accessible and effective than earlier models with similar uses.

Most of the nefarious uses for tracking devices can be prosecuted under existing statutes. Virtually every state already has laws to prohibit the use of tracking devices for stalking or other surveillance.\textsuperscript{xcii} However, if the usage of electronic devices in these cases is limited, as the limited national reporting and dearth of data collection suggest, states may lack case law and precedents for prosecuting crimes involving these devices.\textsuperscript{xciii}

Manufacturers have also worked to minimize risks through technological fixes and cooperation with law enforcement.\textsuperscript{xciv} However, any mitigation measures are likely to require vigilance on the part of potential victims. Users should be aware of their surroundings, inspect belongings, and report suspicious activity.\textsuperscript{xcv}

Reported criminal activity related to tracking devices has primarily consisted of stalking and surveilling vehicles for potential theft. With the reporting on the phenomenon reliant on anecdotal evidence, there is a debate on how widespread and concerning it is currently and what else tracking devices could be used for. One “fact-checking” website noted that local reports are often embellished or taken out of context to make the risks appear greater than they are.\textsuperscript{xcvi} Elsewhere, commenters of a cybersecurity blog noted that with the devices so easy to conceal, the relatively small number of police reports which surfaced in the media could be only a fraction of the actual incidents.\textsuperscript{xcvii}

Evidence of usage beyond local crimes, which would be most concerning for national security, is severely limited. However, it is not hard to imagine that tracking devices used for stalking victims of domestic violence could also be used to track targets for assassination or political violence. The
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALY AVAILABLE TECHNOLOGIES

type of GPS tracking previously seen by well-resourced DTOs could be copied on a smaller scale by other criminal groups.
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALLY AVAILABLE TECHNOLOGIES

HYBRID WARFARE — also known as grey zone conflict or low-intensity conflict — is a reality that the US government, military and private sector must be ready to confront and deter. Hybrid warfare occurs when the online world uses kinetic or physical tools with malicious intent. Hybrid warfare can be used to inflict damage on an adversary in an optimal manner and can include disinformation and malign influence operations, troop movements, disinformation campaigns, cyberattacks or a combination of all these things. Many of the aforementioned technologies, particularly digital platforms and AI, may be used by non-state actors in an attack, namely cyberattacks, such as the use of ransomware.

CONCLUSION: This deliverable answered the aforementioned key intelligence questions as a guide to identify which non-state actors try to acquire commercially available technology that could threaten US interests. The key intelligence questions also guided the team in identifying which novel technologies have the potential to threaten US economic, security, military and space systems. And lastly, the key intelligence questions provided opportunity to address why and how non-state actors pursue the use of existing or advanced technology.  

While most of the commercially available technologies mentioned in this paper, particularly UAS, AM and digital platforms, include real world examples, not all the technologies are exploited equally or by the same type of non-state actors. Non-state actors, such domestic extremists versus international terrorists have different goals and methods to achieve these goals. Similarly, transnational criminal organizations tend to have more financial means to obtain any or all of these commercially available technologies compared to lone actors.

The US Government, intelligence community, and law enforcement at all levels have extensive hurdles to overcome as new technology is developed, or simply as existing technology is adopted by more non-state actors. The purpose of this paper was to address risks from non-state actors’ use and exploitation of some of these technologies. A pending 2023 AEP white paper, authored by the same team, will help address how to counter the use of these commercially available technologies by non-state actors. It is important to note that no single government or industry partner is responsible for these counter-efforts. Instead, many opportunities exist for public-private cooperation to manage the technical, legal, and regulatory challenges stemming from this type of non-state actor use of commercially available technology.
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIAL AVAILABLE TECHNOLOGIES

iii DHS’s Cybersecurity & Infrastructure Security Agency (CISA) developed a Mis-, Dis-, and Malinformation (MDM) team charged with building national resilience to MDM and foreign influence activities. Through these efforts, CISA helps the American people understand the scope and scale of MDM activities targeting elections and critical infrastructure, and enables them to take actions to mitigate associated risks.  
v Verdict | Quora hack reaction: ‘No sector is safe’ as 100m users’ data stolen | 2018 | https://www.verdict.co.uk/quora-hack-reaction/.  
vi Verdict | Quora hack reaction: ‘No sector is safe’ as 100m users’ data stolen | 2018.  
xvi EU Disinfo Lab | The Few Faces of Disinformation | 2022.  
xvii US Department of Justice | Social Media Influencer Charged with Election Interference Stemming from Voter Disinformation Campaign | 2021.  
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALLY AVAILABLE TECHNOLOGIES

xxi Site Intelligence Group | “Azov Battalion Announces New Cryptocurrency and IBAN Options for International Donors” | February 26, 2022.
xxv The Washington Times | 1002/ae85d752-b320-4e19-8285-75c7a1273995 | GUIDE ID: 1002/ae85d752-b320-4e19-8285-75c7a1273995 | 27 November 2018 | New York woman pleads guilty to money laundering to support ISIS.
xxvi Newsday (New York) | STVO-CWP1-DY2H-J3TN-00000-00 | GUIDE ID: 1002/6c7b9d0d-25be-452a-9df2-d5642431f42b | 27 November 2018 | Guilty plea to aiding ISIS.
xxx Department of Justice | “Member of Hacking Group Sentenced for Scheme that Compromised Tens of Millions of Debit and Credit Cards: Damage to Banks, Merchants, Card Companies, and Consumers Estimated at more than $1 Billion” | https://www.justice.gov/opa/pr/member-hacking-group-sentenced-scheme-compromised-tens-millions-debit-and-credit-cards | 7 April 2022.
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALY AVAILABLE TECHNOLOGIES

xxvii Forbes | https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scamb-a-ceo-out-of-243000/?sh=73de610a2241 | Accessed 2022
xiii US Department of Justice | “Ohio Man Pleads Guilty to Plotting July 4th Attack in Cleveland as Part of Plot to Provide Support to Al Qaeda” | 5 November 2019.
xiv US Department of Justice | “Federal Jury Convicts High-Level ISIS Member of Providing Material Support to a Foreign Terrorist Organization, Including Two Counts Resulting in Death” | 25 May 2022.
xv Stanley Center for Peace and Security | “The Gray Spectrum: Ethical Decision Making with Geospatial and Open Source Analysis” | July 2019
xvii Politico | “Meet the Nuclear Sleuths Shaking Up US Spycraft” | 19 January 2022
xviii MITRE | “A Look at Commercial Geospatial Intelligence” | October 2020
xix The Economist | “Open Source Intelligence Challenges State Monopolies on Information” | 10 August 2021
lix The Economist | “Open Source Intelligence Challenges State Monopolies on Information” | 10 August 2021
xlii Welt | “RAF Wanted to Kill Strauss With a Model Airplane” | 23 September 2008
xliv Jane’s Intelligence Review | “Attack of the Drones: The Dangers of Remote Controlled Aircraft” | December 2011
lvi The RUSI Journal | “The Right’s Time to Fly: Exploring the Possibility of Right-Wing Extremists Use of UAVs” | 26 April 2021
lviii US Department of Justice | “Northampton County Man Sentenced to Five Years for Using Drone to Harass Ex-Girlfriend, Illegally Possessing Bombs and Guns” | 24 September 2020
lix War on the Rocks | “Mexican Cartels are Embracing Aerial Drones and They’re Spreading” | 11 November 2021.
lx Judicial Watch | “Mexican Cartels Fly 9000 Flights Into US to Surveil Law Enforcement Operations” | 12 April 2022.
ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALLY AVAILABLE TECHNOLOGIES

---

National Consortium for the Study of Terrorism and Responses to Terrorism (START) | “Motivations, Mechanisms and Determinants of Terrorist Technology Transfer” | 1 October 2017


US Department of Justice | “Affidavit of Special Agency Gary S. Cacace” | 28 September 2011

Cybersecurity and Infrastructure Security Agency | “Recognize Suspicious Unmanned Aircraft Systems” | No Date.


FBI | “Additive Manufacturing” presentation | 6 May 2022.

FBI | “Additive Manufacturing” presentation | 6 May 2022.


FBI | “Additive Manufacturing” presentation | 6 May 2022.


ADDRESSING RISKS FROM NON-STATE ACTORS’ USE OF COMMERCIALY AVAILABLE TECHNOLOGIES

[lxxvi] See for example: Fox 2 Detroit | "Apple Air Tags Being Used to Track Cars and Stalk Victims, Police Warn" | 13 January 2022, News 10 (Albany, NY) | "Police Warn Drivers to Watch Out After Apple 'AirTag' Trackers Are Used to Stalk and Steal" | 23 December 2021; Vice | "Police Records Show Women Are Being Stalked With Apple AirTags Across the Country" | 6 April 2022
[lxxvii] Insight Crime | "Basic Trafficker Technology Trumps Hi-Tech Authorities" | 11 May 2017
[lxxix] The Verge | "Airtags Are Dangerous - Here’s How Apple Could Fix Them" | 1 March 2022
[x] Audrey Kurth Cronin | Power to the People: How Open Technological Innovation is Arming Tomorrow’s Terrorists | 2020.
[xi] The twelve characteristics are: Accessible, Cheap, Simple to use, Transportable, Concealable, Effective, Multi-use, Not cutting-edge (in their second or third wave of development), Bought off-the shelf, Part of a cluster of other emerging technologies, Symbolically resonant, and Given to unexpected uses
[xii] National Conference of State Legislatures | "Private Use of Location Tracking Devices: State Statutes" | 14 February 2022
[xiii] North Carolina Criminal Law | "Cyberstalking via Electronic Tracking Device" | 7 December 2021
[xiv] Apple | "An Update on AirTag and Unwanted Tracking" | 10 February 2022
[xvi] Snopes | "Were Apple AirTag Trackers Being Used by Stalkers?" | 4 February 2022
[xvii] Schneier on Security | "AirTags Are Used for Stalking Far More Then Previously Reported" | 8 April 2022