2023 PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

Addressing Risks From

NON-STATE ACTORS' USE OF COMMERCIALLY AVAILABLE TECHNOLOGIES

Homeland Security

TABLE OF CONTENTS

Executive Summary

The US government (USG) and private sector are working to address the risks posed by non-state actors'[1] harmful use of some commercially available technologies. Technologies of particular concern include fast-growing artificial intelligence (AI), digital platforms, unmanned systems (UxS), and additive manufacturing (aka 3D printing). Some non-state actors are using these technologies at an increasing rate and countering illicit use of these technologies requires a multi-faceted approach and public-private cooperation. Along with lowering barriers to entry, using these commercially available technologies, some non-state actor criminal/terrorist groups can leverage readily available technologies with highly skilled/trained cadre of personnel in low-wage jurisdictions allowing for the ability and cost to conduct an attack to be disproportionately lower than the cost of defending against one.

This DHS-sponsored Analytic Exchange Program (AEP) 2023 Phase II deliverable focuses on AI, digital platforms, UxS, and additive manufacturing, providing a high-level overview of the risks of non-state actor use of these technologies, government and industry responses to those challenges, collaborative public-private efforts, and balancing considerations for the US government. This year's deliverable is designed to build and complement the team's AEP Phase I deliverable which identified risks associated with non-state actors' acquisition and use of a broader range of commercially available technologies[2]. The featured technologies were chosen through multiple team brainstorming sessions, presentations by subject matter experts, and independent research. The four technology groups of concern were identified and selected as being accessible (or commercially-off-the-shelf) and of key interest to various non-state actors; have already been pursued, tested, or fielded by such actors; and/or hold great potential for them to acquire and likely use them in the future. To advance discussions, this Phase II deliverable focuses on risk mitigation recommendations, including those that touch on legislation, policies, regulations, end-user agreements, awareness campaigns, and public education for the US government to consider.

[1] Non-state actor refers to criminal, domestic terrorism, or international terrorism threat actors, not at the direction of a specific nation state.

[2] DHS AEP 2022 Deliverable, *Addressing Risks from Non-State Actors' Use of Commercially Available Technologies,* available at https://www.dhs.gov/publication/2022-aep-deliverables

Team Members

Member	Title and Organization
Clare A.	Intelligence Analyst, Amazon
Rachael C.	Lead Security Monitoring and Response Analyst, Fusion Center, Mastercard
Michael D.	Private Sector
Madeline O.	Senior Analyst, Intelligence and Global Security - Carnival Corporation & PLC
Stephanie P.	Intelligence Analyst, FBI
Don R.	West Point's Combating Terrorism Center
Anissa T.	Intelligence Analyst, NCIS
Team Champion: Jason L.	Senior Analytic Services (SAS) Officer, NCTC

SOURCE SUMMARY STATEMENT

The following deliverable includes source information from various subject matter expert interviews (both private sector and government), team members' knowledge and expertise, and recent open-source reporting from January 2022 to August 2023. The team also attended several conferences and events during this timeframe which contributed to the research on the climate of emerging and commercially available technologies as well as government and industry priorities including:

- RSA Conference (AI, digital platforms)
- CES/Consumer Technology Association Conference (AI, UxS, additive manufacturing)
- GEOWeek (AI, UxS)
- GEOINT Service Days: Army (AI)
- Navy League's Sea Air Space Exposition (AI, UxS)
- Meeting with Congressman Mike Ezell, Member of the Committee on Homeland Security
- NCTC Augmenting Reality Workshop (AI, digital platforms)
- Intelligence and National Security Alliance (INSA) Leadership Dinner with LTG Scott Berrier
- INSA and Armed Forces Communications & Electronics Association International (AFCEA) Intel Summit (AI)

SUMMARY REPORT

2023 PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

This graphic summarizes the report's findings for *Addressing Risks from Non-State Actors' Use of Commercially Available Technologies*.

Artificial Intelligence

What is it?

Increasingly capable software with human-like cognitive functionality

What is the risk?

AI tools are rapidly evolving in speed and scope and can be used by non-state actors for nefarious intent

How is it being addressed?

PUBLIC/PRIVATE SECTORS
Provide joint training on data upskilling opportunities and enhanced awareness

US GOVERNMENT
Identifying lessons learned from key industries. Working with industry and academia to enhance new anc current partnerships

Digital Platforms

What is it?

Software-based online infrastructure that brings value by facilitating interactions and transactions between users

What is the risk?

Actors can access information to commit identity fraud, launder money and impersonate someone's identity to hide illicit activity

How is it being addressed?

TECH COMPANIES
Enforce ethical advertisement or restrict ads completely

PRODUCT DEVELOPERS
Require identity authentication

PUBLIC/PRIVATE SECTORS
Provide information security education and awareness

US GOVERNMENT
Regulate usage or provide best practices

Unmanned Systems (UxS)

What is it?

Any unmanned air, ground, surface, or underwater vehicle

What is the risk?

A low barrier-to-entry tool for non-state actors to conduct reconnaissance, surveillance, smuggling propaganda and attacks

How is it being addressed?

DOD
Developing, procuring, and deploying systems to counter UxS

CONGRESS
Introduced several bills to prevent threats by non-state actors using UxSs

DHS
Published resources on detecting UAS

DOJ
Provides protection at national events to counter UAS; FBI forensic exams of recovered UAS

Additive Manufacturing

What is it?

A process technology with output products such as 3D printed weapons and/or guns

What is the risk?

Actors can stay undetected by reducing their logistical footprints by manufacturing items meant to reduce their acquisition detectability

How is it being addressed?

US GOVERNMENT
Regulates the manufacturing process and printer output, required to be serialized

DOS
Requested the removal of certain Liberator files

CALIFORNIA
Required all types of firearms to be serialized

NEW JERSEY
Required a license to print a gun

Homeland Security

Artificial Intelligence

The Risks

The accessibility and sophistication of AI tools will continue to increase rapidly in the coming years, creating ever-evolving challenges for both the private and public sectors on how to safeguard these tools against non-state actors' use and manipulation. Advances in widely available generative AI tools enable rapid and powerful software development, data-related tasks, content creation, and other capabilities, which can be misused by non-state actors for hacking, mis/dis/mal-information, training, and operations, including those that involve use of autonomous systems. Generative AI may be able to help non-state actors design improvised explosive device trigger designs and baseline explosive recipes by providing guidance to untrained/unskilled personnel on how to acquire the necessary components and assemble some rudimentary devices. At a more strategic level, the broad availability of AI tools also lowers barriers to entry and "gives non-state actors the capability to overcome power imbalances" arming these actors with information, tools, and capabilities they would not have otherwise.[iii]

AI tools present other challenges. They enable non-state actors to attack across kinetic and non-kinetic vectors. Parallel to how militaries consider the use of AI across the scale of autonomy, non-state actors can utilize a range of approaches from human deployment of AI software tools to human-in-the-loop deployment of manned and unmanned systems, in both cyber and/or physical attacks. AI can also make non-state actors kinetic "attacks more efficient and lethal."[iii]

These dynamics will present new challenges to the US national security enterprise oriented around speed and scale, complicating detection and responses. Non-state actors can be more agile and can quickly adapt to, and experiment with, new AI capabilities and use cases, affording them forms of advantage compared to state actors, such as the development of boutique weapons or novel attack pathways. This will likely enhance their ability to innovate and surprise. Non-state actors likely will be able to pivot more quickly to newer types of technologies than state actors could, or new use cases for existing technologies, and therefore be difficult to deter, anticipate, and combat.

Generative AI has received the most media intention over the past year. These tools include large language models, the data on which AI is trained, which can be inexpensive; however, training a model to conduct certain tasks along with the computational and electric/water/cooling powers to manage these systems require a immense monetary and infrastructure resources.

The distributed nature of AI technologies, combined with cloud computing, can enable actors with limited resources to leverage hugely powerful tools while expending minimal tactics, techniques and procedures. As a result, speed enabled by AI will be a key point of competition between states and non-state actors. For the US government speed of detection and speed of response are two areas that require focus.

ADDRESSING THE RISKS

Both government and industry are working to address these risks, collaboratively and independently. Enhanced collaboration and a deepening of partnerships between the public and private sectors will be vital in combatting non-state actors' illicit misuse use of AI.

The US government is working to enhance its understanding of how AI tools will be used in creative, resourceful, and unique ways by non-state actors, including those who embrace violence. As part of those efforts, the government should prepare itself to understand how non-state actors are likely to use AI in ways that cross ethical, moral, and operational norms. The government will need to continue to invest in its capabilities to anticipate and identify what those non-state challenges and use cases might be, and how it will be able to either respond to, or mitigate, them in quick and effective ways. This includes heavy internal investments in AI across agencies and programs. This will require that the US government embrace and make aggressive structural, infrastructural, cultural, and skill-based changes across agencies and departments as it adapts to both using AI tools and countering the threat of harmful AI use by non-state actors.

At present, the US government anticipates fraud and mis/dis/mal-information, and while combatting use of generative AI tools will remain a challenge, government, private sector, industry, and academia have already started testing methods to combat such problems.

With much of AI's advancement being driven by the private sector, one way the government is addressing risk is to try and speed up its ability to procure and deploy AI tools. However, both the private sector and government face challenges in navigating the existing complex government procurement system and ensuring externally developed tools can be appropriately adjusted as needed for government use.

Analytically, the US government is beginning to emphasize and enhance the ability of analysts and practitioners to identify and detect AI generated deepfakes and dis/mis/mal-information efforts at a higher speed and scale. In July 2023, the White House took new steps to address the safety concerns and risks of artificial intelligence and plans to work with both political parties to develop AI legislation, which may assist bipartisan efforts in Congress to craft AI rules. Policymakers face growing pressure from consumer advocates and AI ethicists to craft new laws governing the technology, but previous congressional efforts to regulate Silicon

Valley have been derailed by industry lobbying, partisan differences, and competing priorities.[iv] The development of new tradecraft and tools can help practitioners minimize data interpretation errors, especially when tied to timely and critical decisions or government action. As the government navigates this challenge, it can seek and identify lessons learned from key industries and areas that have been operating in data saturated environments where technology and algorithms that enable speed to decision are a core value proposition.

From a regulatory perspective, the federal government is considering regulating some of the hardware building blocks – e.g. semiconductors, and advanced chip sales. However, given the distributed nature of AI tools and non-state actors' ability to access and utilize them, the core software and techniques are and will be widely distributed and extremely hard to control or "put back in the bottle".

Private sector leaders are also discussing the risks of misuse of AI tools as they are developed at the national level. This has been a topic of discussion for years within the AI community and is resurfacing now with the explosive growth of the sector. Similar to the challenges faced by governments, it is extraordinarily difficult for any single company or industry association to stop broader advancements in AI tools when so many others are pushing forward and, in some cases, competing against one another. Additionally, the speed at which AI tools' sophistication and capabilities are advancing are difficult for platforms to keep up with, especially in terms of content moderation and safeguarding. However, many tech companies, including AI developers, have called on the government to increase regulations for social media platforms and AI tools. In July 2023, several major tech companies signed a deal with the US government to establish more guardrails on AI "including the development of a watermarking system to help users identify AI-generated content, as part of its efforts to rein in mis/dis/mal-information and other risks of the rapidly growing technology."

Pairing with White House initiatives, seven of the most influential companies building AI, including Google, Amazon, Microsoft, Meta and OpenAI, have agreed to a voluntary pledge to mitigate the risks of the emerging technology, vowed to allow independent security experts to test their systems before they are released to the public, and committed to sharing data about the safety of their systems with the government and academics..[v] OpenAI CEO Sam Altman has advocated for more regulations by government leaders, though there are open questions if this would also advance OpenAI's business interests as well. Altman has been eager to meet with policymakers around the world, not just in the United States but also in South America, Africa, Europe and Asia, in an effort to encourage and influence the development of AI regulations.[vi]

With private industry AI development, efforts toward regulations can lead to minimizing capabilities which may complicate business competition and further impact one company's desire to work with another. Specific regulations may also lead to healthy competition if one company can develop and sell a better AI product than their competitor.

Deepening government collaboration with industry will be key to stay on top of the latest developments – many of which are being driven by open-source commercial tools in the private sector. Government entities are enhancing the quality of existing partnerships and developing new ones. Creating and developing private and public sector groups at the analyst and management levels can help promote innovation and information sharing on the utilization, power, and capabilities of new AI tools as they emerge.

Joint public-private programs that provide data upskilling opportunities and enhance awareness of AI technologies are a growing avenue. This includes programs such as the Intelligence Community's Public-Private Talent Exchange (PPTE). Further investment in similar programs can enhance collaboration. One model that US Special Operations Command (SOCOM) has developed and used over the past two decades is its liaison network. In 2021, SOCOM's liaison network was expanded to include the deployment of "technology liaison officers" to key tech hubs.[vii] The US Digital Service and US Digital Corps fellowship[3] are also useful models as they aim to build bridges and create mechanisms for collaboration between government and individuals with technical and specialized skills.

Alexandr Wang, chief executive of Scale AI (founded in 2016), which manages approximately 240,000 human AI trainers, has been working with government leaders for a few years, securing lucrative government contracts and collaborating with members of Congress. To date in 2023, Wang twice briefed the new Select Committee providing insight on the issues of AI. Wang's company spent over $1 million on federal lobbying in 2022, according to public disclosures.[viii] Organizations such as Meta, Microsoft, Open AI, General Motors, SAP, Flexport, and the US Army partner with Scale to solve problems with data labeling and annotation, scenario-based model testing and validation, content understanding and contextualization, AI catalog for asset reusability and more.[ix]

Discussions of the regulation or restriction of AI should also include considerations on maintaining and expanding US leadership in the field. Efforts such as the recent establishment of the Department of Defense (DOD) Office of Strategic Capital help to accelerate domestic investments in critical technologies that will help maintain US technological leadership and

[3] The US Digital Corps is a two-year fellowship for early-career technologists with experiences and identities that reflect the diversity of America to join the public servants already at work modernizing and simplifying government services. The program allows junior technologists to work every day to make a difference in critical impact areas including pandemic response, economic recovery, cybersecurity, and racial equity.

enhance the United States' ability to combat state and non-state actors harmful use of emerging technologies including AI.

Strong voices in the government, private sector, and media, have varying views on the level of government regulation that is appropriate for both AI technology development.

Simultaneously, many digital platforms have adopted AI systems that require large language models to operate. As a result, digital platforms and private industry are utilizing more AI technology in their software programs lending to a whole suite of new and commercially available technology for non-state actors to explore and exploit for illicit use.

Digital Platforms

The Risks

Non-state actors have broad access to harness digital platforms to capture and/or expose sensitive data, propagate mis/dis/mal-information, commit identity fraud and money laundering, and communicate discretely to hide illicit activity.

Violent extremists and terrorist groups use social media and messaging platforms to deliver propaganda, recruit and radicalize individuals, incite attacks, and finance and plan their operations.[x] These non-state actors also rely on encrypted messaging services to communicate and prefer smaller platforms as they can more easily circumvent their weaker controls aimed at removing harmful content such as terrorist recruitment or messaging. Some larger platforms have content moderation teams to prevent the spread of extremist or terrorist content, however, many tech companies have considerably down-sized trust and safety teams in the last year in an effort to lower operating costs and to put more onus on social media users to moderate themselves. Additionally, with paid ads, many are accusing tech companies of profiting from terrorist content and lacking incentive to self-regulate. The continued increase in digital platform accessibility and sophistication allows for an increase in the likelihood of abuse. Misuse can often outpace both application and federal policies to safeguard digital platforms, and social media content moderation has become a contentious topic in the media, politics, and the public. In the last year, there have been several challenges to Section 230 of the Communications Decency Act of 1996, which currently protects social media platforms for being held liable for content uploaded by third parties. Although Section 230 was recently upheld by the US Supreme Court, continued legal and legislative pressure on tech companies to regulate their platforms may lead to changes in content moderation in the next several years.

Addressing the Risks

Social media and messaging platforms operate differently and can therefore draw differing opinions in content moderation, amidst the backdrop of the current social media climate in which content moderation rules are consistently in question. Private and public sector entities should consider pairing or merging their efforts to focus on national security vulnerabilities in the online information ecosystem.

While the government restricts usage or disseminates standards of best practice for usage and development, we are heavily reliant on Industry and Academia to step up since non-kinetic technology has no borders. The private sector is currently driving technological development of digital platforms and can therefore help inform the public sector about emerging technologies and their capabilities. Supporting security researchers and bug bounty[4] programs is expediting identification and reporting of zero-day vulnerabilities and/or unintended data exposures.

Without a universal instrument to suppress online terrorist and criminal activities, raising awareness and formulating countermeasures is essential. Even with countermeasures in place, significant gaps will remain in the government's fundamental ability to anticipate, understand, and address the harms from all online services—not just those with monopoly power—while balancing the multiple, competing interests at the heart of many sociotechnical regulatory decisions.[xi]

Many software platforms have evolved and adopted safety and security regulations that help protect the environment for all users while maintaining and protecting constitutional rights, particularly for freedom of speech. However, if tech companies can increase their transparency and reporting of threat streams and trends publicly to prevent and respond to terrorism online, then continued collaboration with government entities will strengthen response times and mitigate the spread of harmful content on digital platforms. Additionally, tech companies with trust and safety teams can continue to utilize AI technology to detect harmful online content or fake accounts, partnered with analyst review.

Many policies have focused on transparency through both the labeling of ads with purchaser information and the creation of online ad libraries while others increase scrutiny of who is

[4] A bug bounty can be defined as a reward offered to a person who identifies an error or vulnerability in a computer program or system. Many IT companies offer bug bounties to drive product improvement and get more interaction from end users or clients. Companies that operate bug bounty programs may get hundreds of bug reports, including security bugs and security vulnerabilities, and many who report those bugs stand to receive awards.

purchasing ads to prevent inauthentic manipulation. The most extreme policies have restricted advertising altogether.

Product developers can continue to focus on strong authentication practices to validate the identity of and build trust with legitimate users, while dispelling deepfakes, bots, and fraudsters or non-state actors that would use their access to this technology for illicit purposes. Know-Your-Customer policies and practices should also continue to authenticate digital identities and identify abusers. In one such successful example, in April 2023, WhatsApp blocked the account of a Taliban leader, effectively dismantling communication with his followers and canceling a raid on an Islamic State hide-out.[xii]

Self-regulation has allowed companies to implement policies that are self-serving, contradictory, or unenforceable; and even well-intentioned measures have proved insufficient without robust deterrents. Moreover, authoritarian and extremist actors have rapidly adapted to changes on online platforms to circumvent these new policies. The *Honest Ads Act* introduced by US Senators Mark Warner (D-VA), Amy Klobuchar (D-MN), and Lindsey Graham (R-SC) claims it will improve disclosure requirements for online political advertisements.[xiii,xiv,xv,xvi,xvii]

To improve the public's fraud detection skills, the public and private sectors are working toward information security education and awareness. Tech Against Terrorism (TAT) is a non-governmental organization established by the United Nations Counter-Terrorism Committee Executive Directorate to forge ties between tech platforms, academia and civil society. TAT has recently launched a knowledge-sharing platform to send out secure alerts when terrorist content is identified. It has also developed outreach and mentoring programs for smaller internet platforms and governments to build resilience against a growing trend of terrorist content online.

Public and private sectors are engaging more to mitigate the risks posed by non-state actors' use of digital platforms. Information sharing between trusted public and private sector relationships is improving detection and response to these agile and less predictable threats from non-state actors.

To combat these threats, organizations may need to conduct research and intelligence analysis paired with exploratory research and development to better understand the vulnerabilities to exploitation of these digital platforms and their potential impacts. With this information, organizations can conduct collaborative "wargaming" and planning to explore a range of possible, potential, and ongoing threats. The knowledge gained from all of these activities could inform future training and best practices to prepare for and address the associated risks and threats. Organizations and government may need to increase their investments in technology related domains, necessitating countries to not only change how they fight, but also evolve their thinking about deterrence. Expanded regulation, policy making, and political solidarity among members could lead to an increasingly more significant and expanded role. Broader government, military, and civilian cooperation might help to disrupt and mitigate some of these threats from non-state actors' continued use of digital platforms in conjunction with broader public awareness.[xviii]

Holistic programs whereby academia merges with government and private sector can be a key approach to providing solutions to these convoluted threats such as non-state actors' use of digital platforms. For example, The DHS S&T Centers of Excellence (COEs) develop multidisciplinary, customer-driven, homeland security science and technology solutions and help train the next generation of homeland security experts. The Office of University Programs (OUP) makes it easy to access academia to conduct basic and applied research. COEs are university-led research and education assets that provide rigorous, objective research to help anticipate and combat challenges facing the Homeland Security Enterprise. The COEs develop countermeasures, mitigation, and prevention approaches and technologies relevant to DHS missions. The COEs are designed to (a) work with and complement DHS research and development programs, including federal laboratories' homeland security research; (b) take advantage of other related federally-sponsored research; and (c) provide outcomes useful to federal, state, and local governments, private sector, and international partners. The COEs leverage extensive public and private networks, provide individualized services to DHS Components, assist with finding needed research and development (R&D) capabilities, and promote technology transfer, transition, and commercialization. COE partners include academic institutions; industry; national laboratories; DHS operational Components; S&T divisions; other federal agencies; state, local, tribal and territorial homeland security agencies; and first responders.[xix] Even more specifically, University of Nebraska Omaha, as a COE, has taken a detailed approach and leading the way on addressing risks of non-state actors' use of technologies such as the metaverse.

Unmanned Systems

The Risks

Unmanned systems (UxS) include air, ground, surface, and underwater platforms. 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. Unmanned aircraft systems (UAS) are commonly known as drones and utilized by various non-state actors at a much higher rate in comparison to unmanned ground and unmanned surface and underwater systems. The rapid increase in the availability and sophistication of UAS represents a significant challenge, as their capabilities progress faster than the ability to assess and mitigate the threat posed by nefarious use of small UAS by non-state actors. While malicious UAS activity occurs primarily outside the United States, particularly in the Middle East with growing activity in Latin America, the US intelligence community, as well as federal, local, state, territorial and triable law enforcement partners have seen an increasing use in the Homeland by careless, clueless and criminal actors attempting to monitor, penetrate secure locations, or move contraband with UxS by conducting smuggling operations across the US southern borders and into state and federal penitentiaries. Particularly concerning has been the threats that these systems pose to critical infrastructure sites. Many domestic actors have begun flying UAS into restricted airspace to acquire protected imagery and geographic layouts and assess vulnerabilities.

Addressing the Risks

The Department of Defense (DOD) in partnership with the Department of Homeland Security is working with multiple agencies across the interagency to counter adversarial use of UAS domestically and abroad. In FY2023, DoD planned to spend at least $668 million on counter-UAS (C-UAS) research and development and at least $78 million on C-UAS procurement. As DoD continues to develop, procure, and deploy these systems, congressional oversight of their use has increased, as well as participation by the US Government to identify, track and defeat illicit UxS threats.

C-UAS technology can employ several methods to detect and mitigate the presence of hostile or unauthorized UAS. Each C-UAS method utilizes different technologies such as electro optic to identify, radar to track and jammers to defeat, but each one has certain domestic restrictions that can make it challenging to use. These methods can be—and often are—combined to provide a more effective, layered detection and mitigation capability.

DoD maintains the lead C-UAS program for OCONUS threats while DHS maintains primary responsibility to counter CONUS-based UAS threats through various programs and initiatives, such as its Science and Technology Directorate's (S&T's) program, which assesses C-UAS technologies both in laboratory and real-world operational environments and assists DHS Components. The program also guides the development of new and innovative technologies to deliver critical C-UAS capabilities to DHS Components.

The US Special Operations Command (SOCOM) maintains the mission of global integrator for C-UAS integration and left of launch OCONUS. In January 2022, SOCOM awarded a 10-year, $1 billion C-UAS integration contract to Anduril Industries. The contract requires the California-based defense technology firm to "deliver, advance, and sustain" counter-drone sensors and systems in a layered configuration wherever the command operates. Along with delivering and deploying the system, Andrunil will also configure it according to the evolving needs of specific missions. The contract also includes designing, prototyping, and developing new counter-UAS technology.[xx]

In April 2022, the White House released the first whole-of-government plan to address UAS threats in the Homeland. Through the Domestic Counter-Unmanned Aircraft Systems National Action Plan, the Administration identified and proposed efforts to protect against nefarious UAS activity, determine who is authorized to take action, and define lawful steps to action. The Administration also called on Congress to adopt legislation which may help close gaps in existing law and policy that currently impede some government and non-federal law enforcement agencies from conducting C-UAS operations domestically. The Administrations hope is that adoption of this pending legislation will help to protect the American people and our vital security interests from illicit UAS.[xxi] The Domestic Counter-Unmanned Aircraft Systems National Action Plan may be key to assigning and organizing all threat responsibilities while also providing mechanisms and guidance on communicating these threats both CONUS and OCONUS.

Congress has made efforts in recent years to address the threats posed by non-state actors' use of UAS. In 2023, Congress introduced several different bills to bolster US capabilities for C-UAS including *Coast Guard Authorization Act of 2023, FAA Reauthorization Act of 2023, Securing Growth and Robust Leadership in American Aviation Act, STOP Illicit Drones Act, National Drone and Advanced Air Mobility Research and Development Act,* and the *Protecting the Border from Unmanned Aircraft Systems Act.*

In March 2023, Congress introduced a bill called the *Stopping Harmful Incidents to Enforce Lawful Drone Use Act* or the *SHIELD U Act*, which would authorize and expand counter-drone activities by state, local, and airport law enforcement, and federal agencies. The bill authorizes law enforcement to carry out C-UAS activities on commercial service airport property to identify, track and defeat threats posed by unmanned aircraft. The Department of Homeland Security (DHS) is also authorized to carry out these activities. The bill would allow DHS and other agencies to contract with other entities to carry out authorized Counter-UAS activities. Additionally, the Federal Law Enforcement Training Center would expand its curriculum to include training on the use of Counter-UAS activities. Further expanding similar training to state, local, tribal, and territorial law enforcement, as well as private sector security agencies could enhance the ability to address risks associated with the illicit or unsafe use of UxS.

The Preventing Emerging Threats Act of 2018 granted DHS statutory authority to counter credible threats from UAS to the safety or security of a covered facility or asset. This authority enables DHS to identify impacted airspace for certain protection and security missions from certain US Government agencies, including US Coast Guard, US Customs and Border Protection, US Secret Service, and Federal Protective Service.[xxii]

The 2018 Act authorized joint DHS-DOJ mission protection including: (1) National Special Security Events, (2) Special Event Assessment Rating events, (3) Supporting state, local, tribal, or territorial law enforcement at certain mass gatherings upon the request of a State's governor or equivalent, and (4) Active Federal law enforcement investigations, emergency responses, or security operations in specified locations and for limited duration (e.g., airport disruption, disaster response, etc.).[xxiii]

DHS and its Cybersecurity and Critical Infrastructure Security Agency (CISA) has published many resources to aid in the detection of illegal UAS activities including information on critical infrastructure challenges associated with the UAS threat, counter UAS security practices, actions to consider for risk mitigation, and messages of facility and organizational preparedness related to UAS incidents.[xxiv]

In October 2020, the Department of Justice (DOJ) announced the protection activities undertaken by the FBI to counter the threat posed by UAS at certain National Special Security Events (NSSEs), Special Events Assessment Rating (SEAR) events, and select mass gatherings throughout the country. DOJ and the FBI publicized protection activities in an effort to deter careless and criminal UAS operators in light of an anticipated increase in enforcement activity in response to the misuse of UAS.[xxv] Additionally, DOJ and the FBI emphasized their commitment to prosecuting drone operators who use unmanned aircraft to facilitate violence citing the five-year prison sentence imposed September 2020 on Jason Muzzicato, who used an unregistered drone to deploy improvised explosives.

State and local regulations vary widely regarding the operation of UAS, which are in some cases duplicative of FAA rules, such as the following categories: 1. anti-voyeurism/surveillance/harassment; 2. protection of public gatherings/critical infrastructure; 3. operation by government; and 4. regulation of purpose of use or physical attributes of UAS.

Efforts to prevent non-state actors' use of UAS internationally has proven much more difficult. The US has for years imposed export control restrictions and sanctions to prevent foreign adversaries, including non-state actors, from obtaining advanced technology and materials. US officials are looking at enhanced enforcement of those sanctions, encouraging companies to better monitor their own supply chains as well as identify the third-party distributors taking these products and re-selling them to non-state actors.[xxvi]

Many private manufacturing companies are promising increased monitoring of technology and parts sales and distribution; however, companies often insist that controlling where these highly ubiquitous parts end up in the global market is difficult for manufacturers.[xxvii]

Continued awareness bulletins from the IC, increased reporting by bystanders, and training law enforcement on unlawful use of UAS will enable swift action to prevent and stop malicious non-state actors' use of these commercially available system. US government agencies and private sector entities can assist working in tandem to monitor and control risks from unlawful UAS use. CISA collaborates with the private sector to share potential vulnerabilities as well as steps to mitigate risk and damage from malicious use. Various companies partner with both the government and other private sector organizations to open channels of collaboration and communication and to develop technologies that will counter UAS threats. For instance, companies such as DroneShield have contracts with both private sector and governmental agencies that conduct field trial evaluations for technological research and can benefit operations in all areas.

Primary considerations surrounding continued innovation and industry growth of UxS could be to adopt collaborative regulations whereby private sector design, manufacturing and distribution allows for safe consumer knowledge and use.

Additive Manufacturing

The Risks

Additive manufacturing (AM), also known as 3D printing, enables non-state actors to evade law enforcement by reducing their identifiable actions during the acquisition phase of some components needed to support their illicit operations and may lower the cost of production for various types of weapons or critical components used to carry out attacks.[xxviii,xxix,xxx] Non-state actors use of AM equipment to create various weapons or parts, including UxS, privately made firearms (PMFs), and improvised explosive devices (IED) components. The ongoing growth of consumer AM services, which often provide more sophisticated equipment and capabilities than commercial off-the-shelf printers, expands opportunities for threat actors to print components for use in the creation of weapons while reducing their logisitical footprints.[xxxi,xxxii] DOJ and Congress share the concern about PMFs and untraceable firearms based on intelligence reports from DHS, the FBI, and the National Counterterrorism Center, which state that AM weapons and untraceable firearms pose a challenge to law enforcement's ability to investigate crimes and that "wide availability of ghost guns and the emergence of functional AM guns are a homeland security threat."[xxxiii]

The Bureau of Alcohol, Tobacco, and Firearms connected PMFs – also known as ghost guns – to 692 shootings in 2021. Privately made firearms are made by a person other than a licensed manufacturer from available parts sold online, making them untraceable. The Bureau of Alcohol, Tobacco, and Firearms (ATF) identified 25,758 PMFs in 2022. The year before, ATF identified 19,344. That's a 33% increase. The ATF has identified more than 10,000 PMFs in the first six months of 2023 alone.[xxxiv] Worth noting, however, is that all 3D-printed firearms are PMFs but not all PMFs are 3D printed. Further, while the process of 3D printing a firearm is generally portrayed to be relatively easy, an individual still requires some technical knowledge and skill. 3D printing firearm components takes days and a lot of post processing and assembly to create a working firearm.

Addressing the Risks

The US federal government does not specifically regulate 3D printers themselves, but rather the manufacturing process and output of those printers. The guidance on this topic is tentative and subject to change, given the evolving nature of the technology.[xxxv] The effectiveness of legislation aimed at prohibiting the possession of computer-aided design (CAD) files for printing or manufacturing firearms is also rather uncertain. These files remain easily available online and – similar to the two decade long and largely futile copyright enforcement efforts by the music and film industries – difficult to remove. Ultimately, online content is difficult to manage and control online.[xxxvi]

The legality of AM firearms depends largely on the state or local jurisdiction in which they are manufactured and/or possessed as well as legislation relative to the following categories[xxxvii]: (1) Manufacturing of firearms may be prohibited or heavily restricted regardless of the method of production; (2) Making firearms for personal use is not prohibited and is not heavily restricted; whereas production of firearms as a business if not a licensed manufacturer is prohibited and restricted; and (3) While legislation has been introduced in both the House and Senate in previous years on 3D printed firearms and untraceable firearms, federal legislation has not made it past the introduction stage.

To determine legality of a 3D printed firearm, it is also important to distinguish between creating instructions on how to make an AM firearm, possessing a copy of such instructions, and building such a firearm for personal or illicit use. In the US, the legality of sharing the files required to print firearms remains unclear and continues to be highly debated in the courts.[xxxviii] In 2013, *Defense Distributed* – an open-source US-based hardware and software organization – released the digital files for the Liberator, the world's first almost entirely AM firearm. The Liberator attracted a great deal of media and law enforcement attention because within 48 hours of being released, the files were downloaded more than 100,000 times.

The US State Department requested removal of certain Liberator files on the ground that they might be in violation of the Arms Export Control Act and International Traffic in Arms Regulations because it could be accessed in countries where the US has embargoed the sale of weapons.[xxxix] However, in *Defense Distributed v. United States Department of State (2015),* counterarguments appealed the ruling on the grounds that it not only violated the Second Amendment to the US Constitution but also that it violated the First Amendment which prevents the government from abridging the freedom of speech.

In 2016, the Fifth Circuit refused to suspend a regulation restricting publication of CAD files that enable the public to print guns or gun parts using just a 3D printer.[xl] Ultimately, the State Department settled and agreed to permit the distribution of blueprints for AM firearms. [xli] However, state attorneys filed suit asserting states rights regarding the issue in response and the case continues to go back and forth in the courts.[xlii]

US federal law permits the unlicensed manufacture of firearms, including those made using a 3D printer, as long as they contain 3.7 ounces of stainless steel per the Undetectable Firearms Act of 1988. Therefore, in the absence of federal regulation, some states have taken actions to further regulate the creation of PMFs.[xliii] In California, anybody manufacturing a firearm is legally required to obtain a serial number for the gun from the state, regardless of how it's made. Federal legislation does not mention or distinguish federal manufacturing licenses. State registered or licensed firearms are specified (i.e. State of New Jersey, Senate No 2465 Introduce April 12, 2018). In New Jersey, an individual must be registered or licensed to manufacture a PMF. New Mexico, Virginia and others are considering bills that would enact similar restrictions.[xliv]

In August 2022, within the Federal Register, DOJ modernized the definition of a firearm through the "Frame or Receiver" Final Rule, which clarifies that parts kits that are readily convertible to firearms are subject to the same regulations as traditional firearms. These regulatory updates aim to curb the proliferation of "ghost guns," 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.[xlvxlvi] Additionally, all firearms made by federally licensed firearms dealers and gunsmiths, including AM firearms, must be serialized to help reduce the number of unmarked and hard-to-trace PMFs. In addition, the new rule reclassifies unfinished gun frames and receivers as firearms under the law (frames and lower receivers were already classified as firearms under the original statute). It requires federally licensed firearms dealers and gunsmiths to have serial numbers added to any unserialized guns and to run background checks before selling kits that contain parts needed to assemble homemade firearms.[xlvii]

Many US allies address the risks associated with AM somewhat differently by criminalizing the possession of the files required to print firearms, making it a criminal offense to manufacture any firearms or ammunition regardless of the method without authorization to do so; or placing a de facto ban on AM firearms if all forms of firearm manufacturing by unauthorized individuals is prohibited.[xlviii]

Other countries take a different stance entirely as it relates to terrorism and specifically to AM including laws that make the "unauthorized possession of blueprints" for "the manufacture of a gun or a major part of a gun on a 3D printer" a crime.[xlix]

As additive manufacturing technologies continue to decrease in price and increase in quality, and with limited existing legislation to curb access or dissemination of the technical information and software required to produce AM firearms, the sometimes haphazard activities of non-state actors and the absence of well-known cases of terrorist use of AM may create a false sense of security.[l]

In addition to legislation restrictions, since 2020 non-state actors have run up against censorship policies by private sector companies that run major technology and digital platforms, many of which prohibit weapons content. As a result, they have been forced to increasingly obscure corners of the internet. One operations hub for most of the AM gun groups — an encrypted chat and file-sharing platform called Keybase—pledged to remove all weapons-related content and told the groups they would be banned.[li]

Law enforcement has worked more closely with private sector to alert 3D printing makerspaces and other businesses and organizations offering consumer 3D printing equipment and services, of the potential for threat actors to exploit such services for printing various weapons, including firearms parts, improvised explosive devices, or illegal production of laboratory equipment for chemical and biological agents intended for illicit use.[lii]

The dual-use potential of AM makes it difficult to limit the expansion of this technology without also curtailing the innovation, commercial sale and many other benefits. Challenges remain for private manufacturers to maintain constitutionally protected freedoms while government regulations and controls focus on protecting innocent civilians from dangerous weapons created from AM printers. Rather than dragging these issues through the courts, the government at federal, state and local levels could benefit from developing closer relationships with the printer manufacturers, distributors, and software companies working in this industry.

Conclusion

Challenges remain of transcending theory into practice in this world where non-state actors have ready access to commercially available technologies. The question also remains of how to operationalize and improve the public's fraud detection skills if the public and private sectors are working toward information security education and awareness. This puts an enormous cognitive weight on the everyday citizen to be informed and have the skills to make instant analysis and judgment. Further, public and private sector will have to address the metrics and ability or inability to measure the success of awareness and resilience efforts.

One major impact if these issues remain unaddressed, is the mis/dis/mal-information attacks will have a resounding impact on society. As indicated in a recent survey of expert views "fake news, misinformation, and disinformation have become some of the most studied phenomena in the social sciences"[liii]; however, possible solutions and programs have been highly controversial with Congress, the judicial system and industry leaders differing on a cohesive way forward.

Much of this overall issue with how to address non-state actors' use of commercially available technologies tends to focus on educating the end-user, consumer, broader general public audience and consumer of news and information; however, challenges also exist with needing to hold the political, media, business, and academic sectors all responsible collectively and not separately. Funding for Think Tanks, academics, and civil society organizations is not terribly robust, nor for some organizations at all sustainable, hence there is competition and conditional information sharing. There is still a large gap between studying and talking about the problem and finding an operational path forward.

Endnotes

[i] Sarah Kreps and Richard Li, "Cascading Chaos: Nonstate Actors and AI on the battlefield," Brookings, February 1, 2022.

[ii] Sarah Kreps and Richard Li, "Cascading Chaos: Nonstate Actors and AI on the battlefield," Brookings, February 1, 2022.

[iii] Sarah Kreps and Richard Li, "Cascading Chaos: Nonstate Actors and AI on the battlefield," Brookings, February 1, 2022.

[iv] The Washington Post | Cat Zakrzewski | "Top tech firms sign White House pledge to identify AI-generated images" | 21 July 2023 | https://www.washingtonpost.com/technology/2023/07/21/ai-white-house-pledge-openai-google-meta/ | Accessed 25 July 2023.

[v] The Washington Post | Cat Zakrzewski | “Top tech firms sign White House pledge to identify AI-generated images” | 21 July 2023 | https://www.washingtonpost.com/technology/2023/07/21/ai-white-house-pledge-openai-google-meta/ | Accessed 25 July 2023.

[vi] Forbes | Johanna Costigan | “OpenAI’s Sam Altman Makes Global Call For AI Regulation—And Includes China” | https://www.forbes.com/sites/johannacostigan/2023/06/13/openais-sam-altman-makes-global-call-for-ai-regulation-and-includes-china/?sh=191272ac1b47.

[vii] National Defense | “SOFIC NEWS: Special Operators Deploying to U.S. Tech Hubs” | 18 May 2021 | https://www.nationaldefensemagazine.org/articles/2021/5/18/special-operators-deploying-to-us-tech-hubs

[viii] Semafor | Louise Matsakis and Kadia Goba | “The 26-year-old CEO who became Washington's AI whisperer” | 30 June 2023 | https://www.semafor.com/article/06/30/2023/the-26-year-old-ceo-who-became-washingtons-ai-whisperer.

[ix] US House of Representative | HHRG-118-AS35-Bio-WangA-20230718.pdf (house.gov) | https://docs.house.gov/meetings/AS/AS35/20230718/116250/HHRG-118-AS35-Bio-WangA-20230718.pdf | Accessed 25 July 2023.

[x] Institute for Security Studies | Karen Allen | “West Africa: Terrorists' Use of Tech in West Africa Must Be Contained” | https://allafrica.com/stories/202209160017.html | 15 September 2022.

[xi] The Center for American Progress (CAP) | “How To Regulate Tech: A Technology Policy Framework for Online Services” | https://www.americanprogress.org/article/how-to-regulate-tech-a-technology-policy-framework-for-online-services/ | 16 November 2021.

[xii] The New York Times | Christina Goldbaum and Safiullah Padshah | 17 June 2023 | “The Taliban Government Runs on WhatsApp. There’s Just One Problem” | https://www.nytimes.com/2023/06/17/world/asia/taliban-whatsapp-afghanistan.html

[xiii] The New York Times | Christina Goldbaum and Safiullah Padshah | 17 June 2023 | “The Taliban Government Runs on WhatsApp. There’s Just One Problem” | https://www.nytimes.com/2023/06/17/world/asia/taliban-whatsapp-afghanistan.html

[xiv] Tech Funnel | Megha Shah | “What is Digital Identity and How Does it Work” | 17 June 2020 | https://www.techfunnel.com/information-technology/what-is-digital-identity/#:~:text=Disadvantages%20of%20Digital%20Identity&text=The%20biggest%20disadvantage%20of%20a,wrong%20hands%20can%20prove%20dangerous

[xv] Security Intelligence | Sue Poremba | “The Biden Administration’s 2023 Cybersecurity Strategy” | 9 May 2023 | https://securityintelligence.com/articles/the-biden-administrations-2023-cybersecurity-strategy/

[xvi] Securing Democracy | Dipayan Ghosh, Lindsay Gorman, Bret Schafer, and Clara Tsao | “The Weaponized Web: Tech Policy Through the Lens of National Security” | https://securingdemocracy.gmfus.org/wp-content/uploads/2020/12/The-Weaponized-Web.pdf

[xvii] Senator Mark Warner | “The Honest Ads Act” | 2019 May | https://www.warner.senate.gov/public/index.cfm/the-honest-ads-act

[xviii] Arizona State University Threatcasting lab | “Future Implications of Emerging Disruptive Technologies On Weapons of Mass Destruction” | https://cyber.army.mil/Portals/3/Documents/Threatcasting/wmds/Threatcasting_WMDs.pdf?ver=gkwNCrMNUKGK4ojCdMCPTg%3D%3D | Accessed 19 July 2023.

[xix] DHS Centers of Excellence | https://www.dhs.gov/science-and-technology/centers-excellence | Accessed 19 July 2023.

[xx] The Defense Post | INDER SINGH BISHT | 26 January 2022 | https://www.thedefensepost.com/2022/01/26/us-special-ops-counter-drone-contract/#:~:text=The%20US%20Special%20Operations%20Command%20%28SOCOM%29%20has%20awarded,in%20a%20layered%20configuration%20wherever%20the%20command%20operates.

[xxi] The White House | “FACT SHEET: The Domestic Counter-Unmanned Aircraft Systems National Action Plan” | 25 April 2023 | https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/ | Accessed 28 June 20223

[xxii] DHS | Counter Unmanned Aircraft Systems Legal Authorities | https://www.dhs.gov/sites/default/files/publications/dhs_cuas-legal-authorities_fact-sheet_190506-508.pdf | Accessed 28 June 2023

[xxiii] DHS | Counter Unmanned Aircraft Systems Legal Authorities | https://www.dhs.gov/sites/default/files/publications/dhs_cuas-legal-authorities_fact-sheet_190506-508.pdf | Accessed 28 June 2023

[xxiv] DHS | UAS and Critical Infrastructure: Understanding the Risk Video | https://www.cisa.gov/resources-tools/resources/uas-and-critical-infrastructure-understanding-risk-video | Accessed 28 June 2023

[xxv] US Department of Justice Office of Publica Affairs | “Department of Justice Forecasts an Increase in Counter Unmanned Aerial Systems (C-UAS) Protection Activities and Criminal Enforcement Actions” | https://www.justice.gov/opa/pr/department-justice-forecasts-increase-counter-unmanned-aerial-systems-c-uas-protection#:~:text=The%20Department%20of%20Justice%20%28DOJ%29%20today%20announced%20the,throughout%20the%20country%20over%20the%20past%20fiscal%20year | 13 October 2020 | Accessed 28 June 2023.

[xxvi] CNN | “CNN Exclusive: A single Iranian attack drone found to contain parts from more than a dozen US companies” | 4 January 2023 | https://www.cnn.com/2023/01/04/politics/iranian-drone-parts-13-us-companies-ukraine-russia/index.html | Accessed 28 June 2023

[xxvii] CNN | “CNN Exclusive: A single Iranian attack drone found to contain parts from more than a dozen US companies” | 4 January 2023 | https://www.cnn.com/2023/01/04/politics/iranian-drone-parts-13-us-companies-ukraine-russia/index.html | Accessed 28 June 2023

[xxviii] Gov.UK | “Take aim, press print.” https://www.gov.uk/government/news/take-aim-press-print | 9 March 2020.

[xxix] John Hornick, J.D. | FBI Law Enforcement Bulletin | “Dangers and Benefits of 3D Printing” | https://leb.fbi.gov/articles/featured-articles/dangers-and-benefits-of-3d-printing | 13 November 2018.

[xxx] Ruby J Chase and Gerald Laporte | U.S. Department of Justice Office of Justice Programs | The Next Generation of Crime Tools and Challenges: 3d Printing | https://www.ojp.gov/pdffiles1/nij/250697.pdf | April 2018.

[xxxi] FBI | “(U) WMD Concerns with Consumer 3D Printing Services and Makerspaces” | 23 December 2022.

[xxxii] International Center for Counterterrorism | Yannick Veilleux-Lepage | “PERSPECTIVE CTRL, HATE, PRINT: Terrorists and the Appeal of 3D-Printed Weapons” | https://www.icct.nl/publication/ctrl-hate-print-terrorists-and-appeal-3d-printed-weapons | 13 July 221.

[xxxiii] 3DPrinting.com| “New US Federal Rule Treats 3D Printed Guns Like Any Other Firearm” | https://3dprint.com/293667/new-us-federal-rule-treats-3d-printed-guns-like-any-other-firearm/

[xxxiv] Insider | Katie Hawkinson | Tens of thousands of 'ghost guns' legally ordered in pieces online and then assembled at home are flooding the United States” | 15 July 2023 | https://www.msn.com/en-us/news/us/tens-of-thousands-of-ghost-guns-legally-ordered-in-pieces-online-and-then-assembled-at-home-are-flooding-the-united-states/ar-AA1dUaAO.

[xxxv] https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2022/07/fdas-regulatory-framework-for-3d-printing-of-medical-devices-needs-more-clarity#:~:text=FDA%20does%20not%20regulate%203D,output%20is%20a%20medical%20device.

[xxxvi] International Centre for Counter-Terrorism | Yannick Veilleux-Lepage | “CTRL, HATE, PRINT: Terrorists and the Appeal of 3D-Printed Weapons” | 13 July 2021 | https://www.icct.nl/publication/ctrl-hate-print-terrorists-and-appeal-3d-printed-weapons | Accessed 29 June 2023

[xxxvii] International Centre for Counter-Terrorism | Yannick Veilleux-Lepage | “CTRL, HATE, PRINT: Terrorists and the Appeal of 3D-Printed Weapons” | 13 July 2021 | https://www.icct.nl/publication/ctrl-hate-print-terrorists-and-appeal-3d-printed-weapons | Accessed 29 June 2023

[xxxviii] International Centre for Counter-Terrorism | Yannick Veilleux-Lepage | "CTRL, HATE, PRINT: Terrorists and the Appeal of 3D-Printed Weapons" | 13 July 2021 | https://www.icct.nl/publication/ctrl-hate-print-terrorists-and-appeal-3d-printed-weapons | Accessed 29 June 2023

[xxxix] International Centre for Counter-Terrorism | Yannick Veilleux-Lepage | "CTRL, HATE, PRINT: Terrorists and the Appeal of 3D-Printed Weapons" | 13 July 2021 | https://www.icct.nl/publication/ctrl-hate-print-terrorists-and-appeal-3d-printed-weapons | Accessed 29 June 2023

[xl] Harvard Law Review | "Defense Distributed v. United States Department of State" | April 2017 | https://harvardlawreview.org/print/vol-130/defense-distributed-v-united-states-department-of-state/ | Accessed 29 June 2023

[xli] International Centre for Counter-Terrorism | Yannick Veilleux-Lepage | "CTRL, HATE, PRINT: Terrorists and the Appeal of 3D-Printed Weapons" | 13 July 2021 | https://www.icct.nl/publication/ctrl-hate-print-terrorists-and-appeal-3d-printed-weapons | Accessed 29 June 2023

[xlii] Office of the New York State Attorney | "Attorney General James Fights to Protect New Yorkers from Out-of-State Lawbreaker Seeking to Flood Streets with Dangerous Ghost Guns" (ny.gov)| 25 February 2021 | https://ag.ny.gov/press-release/2021/attorney-general-james-fights-protect-new-yorkers-out-state-lawbreaker-seeking| Accessed 29 June 2023

[xliii] The Trace | Champe Barton and Chip Brownlee | "What Are 3D-Printed Guns, and Why Are They Controversial?" | 2 February 2021 | Updated 8 April 2022 | https://www.thetrace.org/2021/02/3d-printer-ghost-gun-legal-liberator-deterrence-dispensed/ |

[xliv] The Trace | Champe Barton and Chip Brownlee | "What Are 3D-Printed Guns, and Why Are They Controversial?" | 2 February 2021 | Updated 8 April 2022 | https://www.thetrace.org/2021/02/3d-printer-ghost-gun-legal-liberator-deterrence-dispensed/

[xlv] US Department of Justice | Press Release | "Justice Department Announces New Rule to Modernize Firearm Definitions" | 11 April 2022 | https://www.justice.gov/opa/pr/justice-department-announces-new-rule-modernize-firearm-definitions | Accessed 29 June 2023

[xlvi] Bureau of Alcohol, Tobacco, Firearms and Explosives | Definition of "Frame or Receiver" and Identification of Firearms | https://www.atf.gov/rules-and-regulations/definition-frame-or-receiver | Accessed 29 June 2023

[xlvii] https://3dprint.com/293667/new-us-federal-rule-treats-3d-printed-guns-like-any-other-firearm/

[xlviii] International Centre for Counter-Terrorism | Yannick Veilleux-Lepage | "CTRL, HATE, PRINT: Terrorists and the Appeal of 3D-Printed Weapons" | 13 July 2021 | https://www.icct.nl/publication/ctrl-hate-print-terrorists-and-appeal-3d-printed-weapons | Accessed 29 June 2023

[xlix] Global Network on Extremism & Technology | Muhammad Faizal Abdul Rahman | "3D-Printed Gun Laws: Girding for the Future of Terrorism" | 28 January 2021 | https://gnet-research.org/2021/01/28/3d-printed-gun-laws-girding-for-the-future-of-terrorism/ | Accessed 29 June 2023

[l] International Centre for Counter-Terrorism | Yannick Veilleux-Lepage | "CTRL, HATE, PRINT: Terrorists and the Appeal of 3D-Printed Weapons" | 13 July 2021 | https://www.icct.nl/publication/ctrl-hate-print-terrorists-and-appeal-3d-printed-weapons | Accessed 29 June 2023

[li] The Trace | Champe Barton and Chip Brownlee | "What Are 3D-Printed Guns, and Why Are They Controversial?" | 2 February 2021 | Updated 8 April 2022 | https://www.thetrace.org/2021/02/3d-printer-ghost-gun-legal-liberator-deterrence-dispensed/

[lii] FBI | "(U) WMD Concerns with Consumer 3D Printing Services and Makerspaces" | 23 December 2022.

[liii] HARVARD KENNEDY SCHOOL | SHORENSTEIN CENTER ON MEDIA, POLITICS, AND PUBLIC POLICY | "A survey of expert views on misinformation: Definitions, determinants, solutions, and future of the field | HKS Misinformation Review (harvard.edu) | https://misinforeview.hks.harvard.edu/article/a-survey-of-expert-views-on-misinformation-definitions-determinants-solutions-and-future-of-the-field/?ref=disinfodocket.com | 27 July 2023