Virtual Plotters. Drones. Weaponized AI?: Violent Non-State Actors as Deadly Early Adopters

Daveed Gartenstein-Ross, Matt Shear & David Jones
Published November 2019

ABOUT THE AUTHORS

Dr. Daveed Gartenstein-Ross is the chief executive officer of Valens Global, a private firm that in both 2018 and 2019 was named to *Entrepreneur Magazine*'s E360 list of small businesses that are mastering the art and science of growing a business, and also leads its sister company Valens Labs, which harnesses the power of artificial intelligence to address critical national-security challenges. He is a scholar, practitioner, and entrepreneur whose work on the intersection of terrorism and new and emerging technologies has been widely recognized, leading the *International Herald Tribune* to describe him as "a rising star in the counterterrorism community."

Dr. Gartenstein-Ross's previous positions include senior advisor to the director of the U.S. Department of Homeland Security's Office for Community Partnerships, fellow with Google's think tank Jigsaw, adjunct assistant professor in Georgetown University's Security Studies Program, and senior fellow at the Foundation for Defense of Democracies.

Dr. Gartenstein-Ross has testified on his areas of core competency before the Canadian House of Commons, and also before the U.S. Senate and House of Representatives over a dozen times. He has served as an expert witness on terrorism and sub-state violence in numerous legal cases in U.S. federal courts, both criminal and civil, and is a featured speaker at events throughout the globe.

The author or volume editor of twenty-three books and monographs, Dr. Gartenstein-Ross has a book forthcoming from Columbia University Press that explores how terrorist groups engage in organizational learning. He has published widely in the popular and academic press, and is a member of the Editorial Board of the leading peer-reviewed journal *Studies in Conflict & Terrorism*.

Dr. Gartenstein-Ross holds a Ph.D. in world politics from the Catholic University of America and a J.D. from the New York University School of Law, and recently earned a Certificate in Entrepreneurship through the Goldman Sachs Foundation's 10,000 Small Businesses program. He speaks five languages.

Matt Shear is an analyst at Valens Global, where he analyzes a broad array of emerging threats, with a focus on the MENA region, Southeast Asia, and West Africa. He is also interested in the challenges posed by domestic extremists across the ideological spectrum. Shear has language skills in both Modern Standard and Levantine Arabic.

Shear graduated Phi Beta Kappa from the University of North Carolina at Chapel Hill, with majors in Peace, War, & Defense and Psychology, and a minor in Arabic. He has conducted research for Dr. Charles Kurzman's annual report on "Muslim-American Involvement with Violent Extremism" and for the START Center's Profiles of Individual Radicalization in the United States (PIRUS) project.

Shear has also interned with the U.S. Marshals Service New York/New Jersey Regional Fugitive Task Force and the Anti-Defamation League.

David Jones is a Senior Researcher with the Organization for the Prevention of Violence, based in Edmonton, Canada. He previously interned for Valens Global in 2016-17.

Jones's research has focused on evaluating the design and implementation and counterterrorism and countering violent extremism (CVE) programming. He has presented his research before diverse audiences, including at the Brookings Institution, Oxford University, the United Nations Safe Cities initiative. He has also served as an instructor for the RCMP's Counterterrorism Information Officer Course.

Jones is a graduate of the University of Alberta.

All three authors would like to express their appreciation of Canada's Department of National Defence, which funded this study through its Targeted Engagement Grant program.

Table of Contents

Executive Summary

Over the past decade, violent non-state actors' (VNSAs) adoption of new technologies that can help their operations have tended to follow a recognizable general pattern, which this study dubs the *VNSA technology adoption curve*: As a consumer technology becomes widely available, VNSAs find ways to adapt it to their deadly purposes. This curve tends to progress in four stages:

1. *Early Adoption* – The VNSA tries to adopt a new technology, and disproportionately underperforms or fails in definable ways.

2. *Iteration* – The consumer technology that the VNSA is attempting to repurpose undergoes improvements driven by the companies that brought the technology to market. These improvements are designed to enhance consumers' experience and the utility that consumers derive from the technology. The improvements help the intended end user, but also aid the VNSA, which iterates alongside the company.

3. *Breakthrough* – During this stage, the VNSA's success rate with the new technology significantly improves.

4. *Competition* – Following the VNSA's seemingly sudden success, technology companies, state actors, and other stakeholders develop countermeasures designed to mitigate the VNSA's exploitation of the technology. The outcome of this phase is uncertain, as both the VNSA and its competitors enter relatively uncharted territory in the current technological environment. The authorities and VNSA will try to stay one step ahead of one another.

This report begins by explaining the adoption curve, and more broadly the manner in which VNSAs engage in organizational learning. The report then details two critical case studies of past VNSA technological adoption to illustrate how the adoption curve works in practice, and to inform our analysis of VNSA technological adoptions that are likely in the future. The first case study is VNSAs' use of social media, culminating in significant recruitment successes and the development of the "virtual plotter" model of terrorism. Daesh in particular has proven uniquely capable of driving attacks by relying on operatives who combine social-media communications with end-to-end encryption designed to bolster their operational security. We trace the development of Daesh's use of virtual plotters, members of its bureaucratic structure who brought to the online space the vast majority of functions that physical terrorist networks used to perform. They scouted for recruits, worked to radicalize them, spurred them to carry out attacks, helped them select their targets and timing of their strikes, and provided technical assistance, all through web-based communication platforms.

Our second case study focuses on VNSAs' use of drones. We explain how a range of VNSAs—including Daesh and al-Qaeda-aligned Hayat Tahrir al-Sham (HTS), Mexico's cartels, and various other groups—are increasingly adopting drones to gather intelligence, move contraband, film propaganda, surveil the battlefield, and carry out attacks.

Virtual plotting and VNSA drone warfare are only two parts of an evolving operational environment that is influenced in large part by new technologies being made available, made cheaper, or simply improved. As a wide range of technologies become more widely adopted at the consumer

level, we must anticipate how VNSAs will acquire, exploit, and improve upon these technologies. Accordingly, based on the adoption curve that this report introduces, we discuss how VNSAs may continue capitalizing on improvements in consumer drones, as well as how they may begin using, or make increasing use of, artificial intelligence and cryptocurrency:

- VNSAs will continue to incorporate unmanned aerial systems (UAS, also known as drones) into their arsenals. The price of drones will continue to fall, and drone platforms will likely undergo advances in propulsion, payload, and maneuverability that enhance their utility to VNSAs.

- VNSAs will likely incorporate artificial intelligence (AI) into all aspects of their operations. This includes recruiting, financing, surveillance, and attack planning. VNSAs may also use AI to expand their illicit activities, particularly in the realms of social engineering and cyber-attacks. This report's discussion of AI separates its applications by whether they are likely to be used by VNSAs, or are merely possible, within the next five years.

- VNSAs' use of cryptocurrencies is contingent in some theaters on the extent to which these currencies can be utilized in mainstream financial transactions. If cryptocurrencies continue to rise in popularity and purchasing power, VNSAs will likely increasingly use them to anonymously procure goods and services and pay personnel, and perhaps find additional uses for them. However, we anticipate that current limitations to VNSAs' employment of cryptocurrencies will not be entirely overcome within the next five years.

Introduction

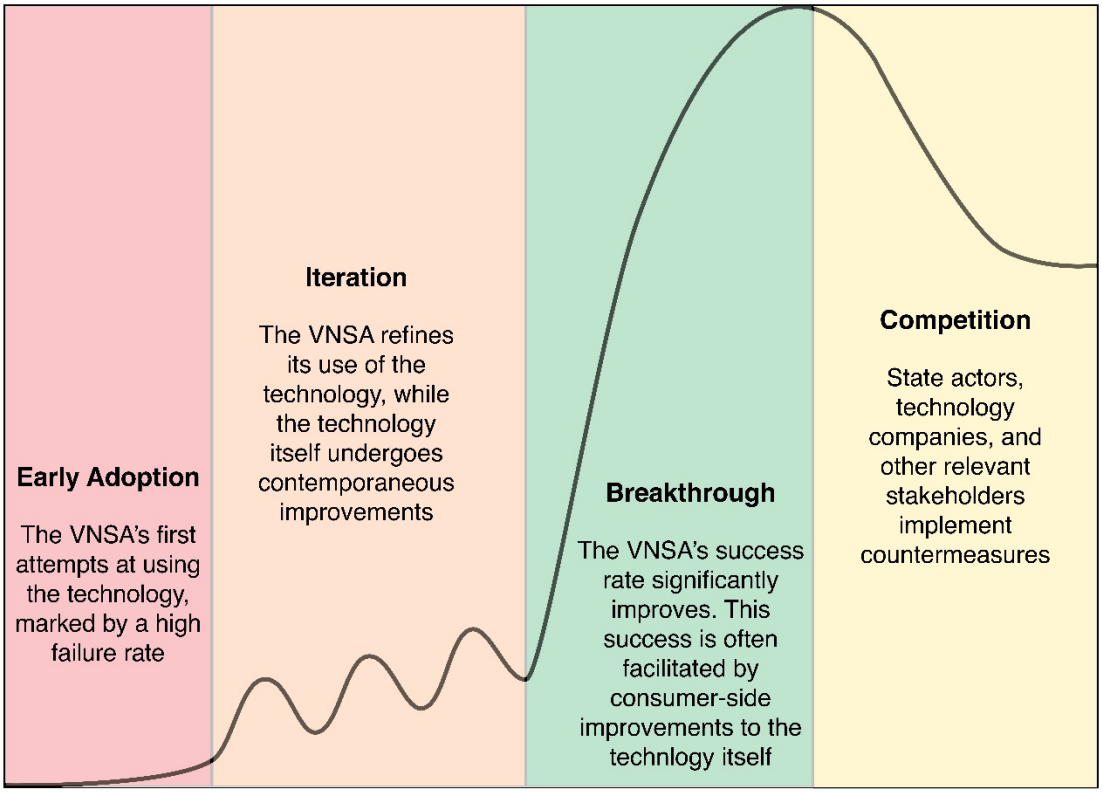
Despite the austere environments in which violent non-state actors (VNSAs) often operate, they rely heavily on modern technologies in their operations. As new technologies emerge, or old technologies change and improve, VNSAs may attempt to adopt them to enhance their operations or expand the range of their activities. Adoption of new technologies is driven by VNSAs' ability to engage in organizational learning. We find that VNSAs' process of technological adoption typically follows an identifiable pattern.

We refer to this pattern as the *VNSA technology adoption curve*. It consists of four phases. The first phase, *early adoption*, is marked by a VNSA attempting to adopt a new technology, and disproportionately underperforming, generally even failing, in important ways. The second phase is *iteration*, during which the consumer technology that the VNSA attempts to repurpose to advance its aims undergoes iterations or improvements driven by the companies that brought the technology to market. These improvements are designed to enhance the experience of, and utility to, the consumer. The improvements help the intended users, and also aid the VNSA, which similarly iterates with the technology. The third phase is *breakthrough*, where the VNSA's success rate with the technology significantly improves. The final phase is *competition*, where the VNSA's adversaries adapt to counteract its breakthrough: Technology companies, state actors, and other stakeholders are compelled to develop countermeasures. The contours of this phase are difficult to anticipate, as both the VNSA and authorities enter uncharted territory in the current technological environment. The VNSA and its foes try to stay one step ahead of one another while technology plunges ahead apace.

It is not inevitable that a VNSA's attempts to adopt a technology will ultimately succeed after initial efforts fall short. Nor is it inevitable that a VNSA will fail in the earliest stages of adopting a new technology. Sometimes its first effort is a stunning success—often followed by a series of disappointing second acts, as the VNSA moves into the iteration phase. Thus, our adoption curve should not be understood as deterministic, but rather as a frequently repeated pattern that has explanatory power as a model. We hope that the adoption curve will help practitioners and scholars to avoid misdiagnosing what a VNSA is doing in the early parts of the curve.

Specifically, it is at best overly simplistic, and perhaps outright inaccurate, to see the VNSA's early attempts as "failures," and later third-phase attempts as "successes" in a binary fashion. Indeed, many for-profit firms now perceive the need to bring less-than-perfect products to market, which are generally known as the *minimum viable product* (MVP).[1] In contrast to an earlier technological generation, where a poor initial product could doom a firm's reputation, in the digital space it is now possible for firms to rapidly improve products even after they are in the customer's hands. MVP principles allow a firm to disseminate a product soon after it is viable for consumer use, understand what consumers like and dislike, and rapidly improve the product. Just as it would be wrong to think of the early stages in the MVP process as a firm failing, so too should early attempts in the VNSA adoption curve be understood as transcending success or failure. They are processes of learning and iterating.

[1] See Eric Ries, *The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses* (New York: Crown Business, 2011).



The VNSA technology adoption curve.

This report explores two case studies in detail that illustrate the VNSA technology adoption curve: VNSAs' use of social media to coordinate external operations, and VNSAs' use of unmanned aerial system (UAS; also known as drone) technology. Ideological VNSAs in particular (*e.g.*, Daesh) gravitated toward social media as a platform to spread propaganda and inspire attacks abroad.[2] One early militant propagandist to recognize the power of social media was the Yemeni-American Anwar al-Awlaki, an al-Qaeda in the Arabian Peninsula (AQAP) preacher and external operations commander. Awlaki used sermons posted to YouTube and online magazines to recruit, and to encourage his followers to strike outside of AQAP's core territory. Though Awlaki should be regarded as stunningly successful in his efforts, later recruiters who employed Twitter possessed even greater ability to target their messaging and engage their audience.

Daesh picked up where Awlaki left off, employing other, more interactive social media platforms to reach a wider audience, while fostering "remote intimacy" through one-on-one communications with potential operatives.[3] The group recognized that cultivating remote intimacy

[2] Daesh is the transliterated acronym for the self-proclaimed Islamic State's Arabic name: *al-Dawla al-Islamiyya fi-l-Iraq wa-l-Sham*. The term *Daesh* closely resembles pejorative Arabic words, including *bigot* and *to trample*. This has prompted the Canadian government, among others, to refer to the group as Daesh instead of ISIS or ISIL, which are two other common acronyms employed for it. Using the term Daesh also consciously avoids applying the words *Islamic* and *state* to the group. Though there are solid arguments for various ways of referring to the militant group, we employ the Canadian custom here because the Canadian Department of National Defence sponsored this study.

[3] The phrase *remote intimacy* was coined by J.M. Berger, who explained: "Despite the distance and lack of physical contact that create this safe zone for conversation, it is possible to forge very strong bonds of intimacy online. As the technology migrates from computers to phones, many social media users are 'always on,' a trait which ISIS courts with its

held enormous potential to draw foreign recruits to its core organization in Syria and Iraq, and to inspire external operations. The Daesh officials first assigned to connect with foreign sympathizers in the *iteration* phase often had poor operational security, resulting in a high proportion of their recruits being arrested. The group eventually reached its *breakthrough* phase, marked by successful implementation of its "virtual plotter" model. This model uses online communications to effectively perform the majority of functions previously reserved for physical networks. Daesh virtual plotters communicate with sympathizers across the globe, providing them with detailed strategic, tactical, financial, and sometimes even emotional support. Alarmed by Daesh's success, governments relatively quickly adopted a coordinated response, while social media companies began removing users and content affiliated with the group. This sparked the ongoing *competition* phase between Daesh and its adversaries in the online sphere.

With respect to UAS, significant advances in consumer drone technology likewise allowed VNSAs to integrate them into their arsenals. Early drones were generally unsuitable to VNSAs' purposes for various reasons, including being too expensive, too unreliable, or too complicated. But rapid technological improvements allowed these groups to *iterate* on drones, and they reached a *breakthrough* phase where they were able to exploit drones as they never had before. VNSAs now use drones in myriad ways, including in drug smuggling, aerial bombing, and creating powerful propaganda. To *compete* with this success, drone manufacturers and state security entities have introduced a number of kinetic and technological countermeasures.

To understand VNSAs' technological adoption, it is important to understand these groups' more general processes of organizational learning. The following section examines organizational learning principles and their relevance to VNSAs, before the report turns to a detailed discussion of how VNSAs traversed the technology adoption curve with both social media and UAS. We will then turn to anticipating the ways in which VNSAs may continue to integrate modern technologies—specifically drones, artificial intelligence, and cryptocurrencies.

overwhelmingly active online presence." J.M. Berger, "The Metronome of Apocalyptic Time: Social Media as Carrier Wave for Millenarian Contagion," *Perspectives on Terrorism* 9:4 (2015).

How Violent Non-State Actors Learn

For violent non-state actors (VNSAs), the ability to innovate is a necessity rather than a luxury. Facing an array of internal and external challenges, these groups must be capable of adapting quickly and creatively, or else suffer the consequences. VNSAs that fail to develop coherent responses to counterterrorism, counterinsurgency, or law enforcement policies aimed at capturing or killing their members will eventually be degraded to the point of irrelevance. Similarly, VNSAs that cannot overcome defensive measures aimed at preventing their illicit activity may be rendered obsolete.

In addition to this *innovate or die* imperative, competition among VNSAs is another driver of organizational learning. Competing groups often vie for the same pool of money, recruits and supporters. Those that innovate in the realms of messaging, recruitment, strategies, and tactics will attract resources and support. Those incapable of adapting will watch their support base wither.

Breakthroughs in the technological sphere serve as an accelerant of VNSA organizational learning. The dizzying rate at which new technologies, including communications platforms and consumer products that may be repurposed into weapons systems, are introduced creates significant opportunities for VNSAs. But technological innovation is a double-edged sword, and new technologies also create pressures. For example, as intelligence agencies develop increasingly sophisticated means of monitoring and tracking VNSAs, these groups must devise new communication and operational security techniques, often involving a combination of high-tech and low-tech methods.

Given these challenges, successful VNSAs develop strong learning processes. They generally identify gaps in their capabilities, institutionalize best practices, and become effective innovators. Through these steps, they can improve their chances of success.[4]

The value of knowledge is as true of businesses as it is of VNSAs, and the dynamics of VNSA organizational learning bear close resemblance to learning processes in the business world. For-profit companies generally do not have to contend with state actors trying to eliminate them (though sometimes they do!), but they face many of the same pressures to adapt as do VNSAs. Businesses compete with their rivals to maintain a competitive advantage. Firms must be highly responsive to consumers' changing needs, just as VNSAs must be attuned to the demands of their support base.

Further, the technology boom of the past several decades that has forced VNSAs to engage in constant processes of innovation has had a similar, and likely more dramatic, effect on for-profit companies. Rapid and often unpredictable technological change has placed a premium on learning mechanisms and capabilities. As Rita Gunther McGrath, a respected expert on innovation at Columbia Business School, has explained, "the greater the environmental uncertainty, those organizations that prove to have superior abilities to manage exploration will be better able to adapt to changing circumstances."[5]

---

[4] Cf. George P. Huber, "Organizational Learning: The Contributing Processes and the Literatures," *Organization Science*, February 1, 1991.

[5] Rita Gunther McGrath, "Exploratory Learning, Innovative Capacity and Managerial Oversight," *The Academy of Management Journal* 44:1 (February 2001), p. 119.

Given the similarities between the way that VNSAs and for-profit firms innovate and adapt, the rich literature on organizational learning in the business world provides valuable insight into the drivers, processes, and dynamics that shape how VNSAs learn. The field of terrorism studies has generally understudied relevant theories and concepts from the organizational learning literature, with several notable exceptions.[6]

We begin this section of the report by defining organizational learning and showing how it is distinct from individual learning. We then ask why organizations pursue learning at all, given the high costs of engaging in organizational learning. Finally, we explore the learning processes that VNSAs can draw upon, and the factors that influence the outcome of organizational learning efforts.

Defining Organizational Learning and Innovation

The concept of individual learning is relatively unambiguous, but the notion of learning at the organizational level is less clear-cut. Any description of the concept must show how organizational knowledge obtained by a company employee or VNSA member is distinct from knowledge that an organization accrues as a result of that employee or member's *individual* learning.

The literature identifies several prerequisites for organizational learning. First, processes must be in place to translate knowledge gained at the individual level into organizational knowledge. If knowledge obtained individually is not institutionalized, organizational learning does not occur. Put another way, organizational learning only occurs when knowledge is committed to an organization's memory, such that the organization is "no longer dependent upon the original learner."[7] This process is essential for VNSAs, which typically suffer high levels of attrition. A second defining feature is that organizational learning is greater than the sum of the organization's parts.[8] It is wrong to view organizational learning exclusively as an aggregation of the knowledge gained by various members. Instead, through absorbing, distributing and institutionalizing knowledge across multiple levels of the organization, the initial information gathered by an individual is amplified. Organizational learning is a force multiplier.

---

[6] One such exception is *Aptitude for Destruction*, a two-volume report by Brian Jackson and his colleagues at the RAND Corporation that reviews organizational learning principles that are applicable in the context of terrorist groups and illustrates them through several case studies. Brian Jackson et al., *Aptitude for Destruction, Volume 1: Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism* (Santa Monica: RAND Corporation, 2005) (outlining applicable organizational learning principles); Brian Jackson et al., *Aptitude for Destruction, Volume 2: Case Studies of Organizational Learning in Five Terrorist Groups* (Santa Monica: RAND Corporation, 2005) (exploring case studies). Another contribution is *Understanding Terrorism Innovation and Learning*, a 2015 volume co-edited by Magnus Ranstorp and Magnus Normark that, like RAND's report, reviews the academic literature on learning and innovation, and provides a series of case studies applying these theories to terrorist groups. Magnus Ranstorp & Magnus Normark, *Understanding Terrorism Innovation and Learning: Al-Qaeda and Beyond* (London and New York: Routledge, 2015). Also relevant is Michael Kenney's 2007 volume examining the similarities in success experienced by cartels and jihadist groups through the lens of their ability to learn and store information, as well as adapt to changes in their environment. Michael Kenney, *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation* (Philadelphia: University of Pennsylvania Press, 2007). Most recently, a special issue of the academic journal *Studies in Conflict & Terrorism* published in late 2017 was devoted to organizational learning in terrorist groups; it was titled "How Terrorists Learn: Adaptation and Innovation in Political Violence." But VNSAs' organizational learning undoubtedly merits further scholarly attention.

[7] Mick Beeby & Charles Booth, "Networks and Inter-Organizational Learning: A Critical Review," *The Learning Organization* 7:2 (1994).

[8] Jackson et al., *Aptitude for Destruction, Vol. 1*, p. ix.

Scholars of organizational learning appear to have arrived at a rough consensus on the factors that differentiate organizational from individual learning. But there is no consensus definition of organizational learning itself. We are sympathetic to Louise Kettle and Andrew Mumford's definition in the context of terrorism, where they define such learning as "the acquisition of knowledge to inform terrorist related activities in the future."[9] This definition makes two important contributions as compared to other widely adopted definitions of terrorist groups' organizational learning. First, their definition clarifies that learning need not necessarily result in change. Second, it clarifies that learning will not necessarily produce positive outcomes. Though Kettle and Mumford's definition is focused on terrorism, we believe it is more broadly applicable to VNSAs with a slight linguistic adaptation: *the acquisition of knowledge to inform VNSA-related activities in the future*.[10]

Obstacles and Drivers: Why Do Organizations Learn?

Understanding when and why organizations pursue learning is an important area of scholarly interest. Organizational learning, and the changes that it spurs, can be uncomfortable, especially given most organizations' natural preference for stability over uncertainty. Discontinuous change, which requires organizations to abandon enduring norms and procedures, is particularly difficult. Learning itself can be a costly exercise.

Perhaps a good starting point in addressing this question is examining why organizations *do not* engage in learning. Organizational culture is often the greatest obstacle. As organizations age and become more successful, they become increasingly committed to their norms and practices. Organizational culture can create impediments to learning. Tushman and O'Reilly write that cultural inertia can foster complacency, even arrogance, thus preventing organizations from recognizing the gap between their current capabilities and objectives.[11] Another obstacle relates to organizational size. As organizations expand, they create new layers of procedures and bureaucracy. These modifications improve an organization's ability to implement existing policies and strengthen intra-organizational communication, but also serve as a hindrance to organizational learning, particularly discontinuous learning. To modify policies and procedures, bureaucratized organizations must implement changes across multiple departments. This is a complex undertaking. It is also one reason many large organizations prove resistant to implementing sweeping change, a phenomenon that Tushman and O'Reilly describe as "structural inertia."[12]

Cultural and structural inertia are in part consequences of the tradeoff between exploration and exploitation. In 1991, James March, a scholar of organizational behavior, published a seminal article explaining the exploration-exploitation dynamic. March observed that exploration involved "experimentation with new alternatives."[13] The emphasis on the new in exploration contrasts with exploitation, which seeks to improve the efficiency of an organization through "refinement and

[9] Louise Kettle and Andrew Mumford, "Terrorist Learning: A New Analytical Framework," *Studies in Conflict & Terrorism* 40:7 (2017), p. 530.
[10] In its insights, Kettle and Mumford's definition is similar to that of George Huber, who contends that "an entity learns if, through its processing of information, the range of its potential behaviors is changed." Huber, "Organizational Learning," p. 89. That is, change stemming from organizational learning can be cognitive rather than behavioral, and can result in modifications to an organization's worldview that are not immediately evident to an outside observer.
[11] Michael Tushman and Charles O'Reilly III, "Ambidextrous Organizations: Managing Evolutionary and Revolutionary Change," *California Management Review* 38:4 (1996), p. 18.
[12] Ibid.
[13] James March, "Exploration and Exploitation in Organizational Learning," *Organization Science* 2:1 (1991), p. 85.

extension of existing competences, technologies and paradigms."[14] Though organizations should ideally pursue both types of learning, March discerned a general preference for exploitation. This tendency was a product of firms' desire to improve existing practices, as well as their reluctance to examine unproven alternatives. Other scholars have noted that this dynamic often resulted in short-term improvements, but "diminishing returns to the organization" in the long term.[15] Similarly, in his acclaimed book *The Innovator's Dilemma*, Clayton Christensen examines how even the most well-run companies decline. Christensen argues that in doing everything "right," such as being attentive to short-term market trends, adjusting to customer feedback, and diverting funding to innovations that "promised the best returns," titans who concentrate on incremental improvements can be felled by disruptive innovations.[16]

Individual-level factors may also obstruct organizational learning. Gary Ackerman highlights the role of "guardians of the status quo" in inhibiting learning. These guardians are beneficiaries of an organization's current policies and procedures, and could lose power or influence if the organization changes tack. They thus directly or indirectly deter major adaptations.[17] Competition within an organization can also be an obstacle to learning. Executives or commanders may try to stymie organizational rivals' efforts to engage in exploration.

Even if organizations can overcome these barriers, most VNSAs do not have the resources to constantly evaluate their capabilities. VNSAs must prioritize their own survival, and often lack the luxury of designating personnel to conduct internal assessments. Such groups' deliberate organizational learning is often sparked by a triggering event that reveals the limits of their approach.

The most prominent driver of organizational learning is a dramatic shift in an organization's exogenous environment that leaves it little choice but to innovate or risk decline. One such challenge is the emergence of a rival organization. Competition forces organizations to modify policies and procedures to keep pace with other actors in the same space, who are vying for the same resources. Dramatic technological change can serve as another catalyst for organizational learning.[18] New technologies can render old practices obsolete. Consider the rapid changes in the film industry. For decades, videocassette recorders (VCRs) were a fixture in homes around the world, with stores selling over 200 million units a year at the peak of sales in the mid-1990s.[19] But the widespread adoption of DVDs transformed the VCR from a common household commodity into a vestige of a past era. By the early 2000s, DVD player sales outpaced those of VCRs at a rate of 40 to 1.[20] Online video streaming then reshaped the market once again. Technological innovation has had a similarly transformative effect on VNSAs. Innovations in social media and communications, as well as advances in end-to-end encryption, have reshaped how militants interact with one another. Jihadist

---

[14] Ibid.

[15] Laurence Weinzimer & Candace Esken, "Learning from Mistakes: How Mistake Tolerance Positively Affects Organizational Learning and Performance," *Journal of Applied Behavioral Science* 53:3 (2017), p. 323.

[16] Clayton Christensen, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail* (Cambridge, MA: Harvard Business Review Press, 2000), p. xii.

[17] Gary Ackerman, "The Theoretical Underpinnings of Terrorist Innovation Decisions," in Magnus Ranstorp & Magnus Normark, *Understanding Terrorism Innovation and Learning: Al-Qaeda and Beyond* Kindle ed. (London and New York: Routledge, 2015), loc. 734.

[18] For an extended discussion of the relationship between technological change and organizational learning, see Tushman and O'Reilly, "Ambidextrous Organizations," pp. 8-30.

[19] Robert Uhlig, "DVD Kills the Video Show as Digital Age Takes Over," *The Telegraph* (London), November 22, 2004.

[20] Ibid.

groups in particular have adapted their approaches to recruitment, communications, and external operations to capitalize on these developments.[21]

Sudden political, social and economic shifts can be another driver of organizational learning. Most organizations possess strategies and tactics rooted in existing conditions. When conditions evolve, organizations may be forced to engage in learning. Shifting political dynamics present VNSAs with opportunities as well as challenges.

Though organizations are most likely to be responsive when there are exogenous shifts, endogenous factors can also be catalysts for learning. Changes in leadership may shift strategy. Competition between mid-level officials, while sometimes a hindrance to innovation, can also spur organizational learning as rivals engage in one-upmanship. In these cases, organizational learning may be internally fragmented: Rivals won't share knowledge with one another, resulting in stove-piping and information silos. And highly entrepreneurial individuals, whether at the top echelons of the organization or lower levels, may drive organizational learning on their own. Khalid Sheikh Mohammed, the mastermind of 9/11, was one such individual, spearheading considerable innovation in al-Qaeda's external operations.

Processes of Organizational Learning

Organizations that recognize the need for learning must orchestrate a strategy for obtaining new information and incorporating it into organizational procedures and culture. Learning processes are not uniform, as they depend on numerous internal and external factors.

Scholars have built several frameworks explaining the variables that affect learning processes. One of the more comprehensive frameworks applicable to VNSAs can be found in the study *Aptitude for Destruction*, written by Brian Jackson and his RAND colleagues.[22] Jackson et al. identify four stages of organizational learning processes: acquisition, interpretation, distribution, and storage. While all four stages must be fulfilled for learning to be assimilated and adopted across an organization, the stages do not necessarily occur in a specific order. Organizational learning rarely follows a linear path. Instead, organizations often alternate between acquiring new knowledge, and analyzing and incorporating it into processes. The dynamic nature of organizational learning is even more pronounced for VNSAs, which often lack the operational freedom needed to standardize learning processes.

Acquisition. Acquisition involves the collection of information relevant to a learning objective. Organizations can draw from many sources to obtain knowledge. An organization may watch the behavior of other organizations, a process known as *vicarious learning*.[23] Vicarious learning allows organizations "to acquire large, integrated patterns of behavior without having to form them gradually

[21] We use the term *jihadist* in this report because it is an organic term: the way that those within the movement refer to themselves. However, it should be understood that the Arabic word *jihad*, which means *struggle* in English, is a well-established Islamic religious concept with many connotations. Most Muslims interpret the term in significantly different ways than do self-proclaimed jihadists. For many Muslims, jihad is a peaceful inner struggle to live in accordance with Islam. But Islamist militants who refer to themselves as *jihadists* emphasize the physical warfare aspect of jihad, broadly interpreting when such warfare is justified.

[22] Jackson et al., *Aptitude for Destruction, Vol. 1*.

[23] Ibid., p. 11.

by tedious trial and error."[24] But the depth of vicarious learning may be limited, as often only the public-facing behavior of other organizations can be observed. Direct cooperation with other groups can address some limitations of vicarious learning: A partner organization can provide access to its internal processes and deliberations. But this option may be more limited for VNSAs, for whom partnerships with other organizations can be difficult or even dangerous.

Data repositories—the Internet in particular—serve as another critical source of information for organizations engaged in learning. The Internet provides *explicit knowledge*, information that can be codified and transmitted through written documents, but it is suboptimal for conveying *tacit knowledge*, information difficult to express in written or verbal form that relates to the implementation of an activity.[25]

Organizations can also draw on the existing knowledge of their members. One of the most influential sources is congenital knowledge, the knowledge of an organization's founding members. Initial decisions about an organization's structure, aims and strategy are largely based on the knowledge, decisions, and outlook of the founders, who "incorporate the practices and procedures defined by prevailing rationalized concepts of organizational work."[26]

But perhaps the most valuable source of knowledge is experiential learning. Unlike vicarious learning, experiential learning allows organizations to use trial and error to identify best practices. The effectiveness of experiential learning often depends on an organization's tolerance for risk and failure, as mistakes can be "a rich breeding ground" for experiential learning.[27] The outcome of experiential learning also hinges on an organization's ability to evaluate itself.[28]

Interpretation. In many respects, the interpretation phase is the most significant in the organizational learning process. Information acquired will be largely meaningless unless organizations can successfully analyze and interpret it to determine its significance. Interpretation is also highly subjective, and thus susceptible to organizational and individual biases. Valuable information may be squandered if an organization lacks strong analytic tools.

Numerous factors determine how organizations interpret information. Organizational culture is often a crucial determinant. An organization resistant to change or riven by internal schisms may be incapable of accurate interpretation. Organizational rivals may interpret information to serve their own purposes, even if it comes at the expense of the organization as a whole. Ideological flexibility or rigidity also influences how an organization interprets information. An organization wedded to a certain doctrine may be susceptible to confirmation bias.

Distribution and Storage. The distribution and storage phases facilitate the transition of knowledge from individuals and small groups to the organization as a whole. For organizational learning to occur, knowledge obtained by individuals must be diffused across the organization and committed to its memory. Distribution, where members share knowledge internally, "significantly

---

[24] Mark Dodgson, "Organizational Learning: A Review of Some Literatures," *Organization Studies* 14:3 (1993), p. 386.
[25] See discussion in Kettle and Mumford, "Terrorist Learning," p. 528; Kenney, *From Pablo to Osama*, pp. 135-66.
[26] John Meyer and Brian Rowan, "Institutionalized Organizations: Formal Structure as Myth and Ceremony," *American Journal of Sociology* 83:2 (September 1977), p. 340.
[27] George Romme and Ron Dillen, "Mapping the Landscape of Organizational Learning," *European Management Journal* 15:1 (1997), p. 71.
[28] Huber, "Organizational Learning."

lowers the risk that an organization's learning will deteriorate," and ensures that the knowledge obtained by an individual or small group will be retained even if the individual or group leaves.[29]

The distribution process does, however, stand in tension with the specialization of labor in a bureaucratic organization. Organizations in a growth state will pursue greater specialization to maximize efficiency. Specialization and compartmentalization may reduce the likelihood that information will be shared across an organization. Separate departments may establish information silos, and be unaware that the information they obtain would be valuable elsewhere.[30] The result is redundancy and inefficiencies. Organizations intent on diffusing and institutionalizing knowledge must thus develop information-sharing policies.

Other impediments to distribution may be unique to VNSAs. For instance, the process of distributing knowledge may expose VNSAs' clandestine activities. Distribution requires coordination between different cells and departments. This is generally not problematic for regular firms, but may increase the physical signature of VNSAs and reveal the scope and shape of their networks to state actors. When VNSAs decentralize their networks, a step taken to improve security, it may also complicate distribution.

The storage phase ensures that knowledge that is acquired, interpreted, and distributed throughout the organization is conserved and packaged in such a way that individuals far from the original source of information can benefit from it. Storage often involves the conversion of information from one type of knowledge to another. Mick Beeby and Charles Booth identify three types of knowledge conversion or transfer relevant to the storage phase.[31] *Socialization* refers to the sharing of tacit knowledge within an organization. In-person communication is often required to facilitate the transmission of tacit knowledge, and in some cases organizational culture can serve as a vehicle for conveying tacit knowledge. *Externalization* involves the "conversion of tacit into explicit knowledge through a process of codification."[32] This kind of knowledge conversion is likely to be incomplete. Some information will be lost in the conversion to explicit knowledge because of the sticky and intransigent nature of tacit knowledge. This dilemma is particularly relevant to VNSAs, which must be able to develop mechanisms for converting and transmitting tacit knowledge across relatively decentralized networks. Finally, *internalization* concerns the transfer of explicit into tacit knowledge through routinization. By ingraining explicit knowledge in its cultural DNA, an organization can provide members with crucial information.

Organizational Learning in the VNSA Context

Though the frameworks examined in this section help explain the general drivers and processes of organizational learning, there is no one-size-fits-all model for analyzing how organizations learn. An organization's culture, strategy, structure, and external environment all have an impact.

This raises the question of whether VNSA organizational learning is *sui generis*. It further forces us to consider that VNSA organizational learning is not monolithic. Jihadist groups, for example,

[29] Jackson et al., *Aptitude for Destruction, Vol. 1*, p. 13.
[30] Romme & Dillen, "Mapping the Landscape of Organizational Learning," pp. 66-78.
[31] Beeby & Booth, "Networks and Inter-Organizational Learning," pp. 75-88.
[32] Ibid., p. 78.

differ in critical respects from other VNSAs. They must contend with state security forces and rival actors, while at the same time being cognizant of the needs and interests of local populations. They frequently maintain fluid hierarchies with little resemblance to conventional firm structures. Unlike drug cartels and criminal syndicates, jihadist groups are more ideological than they are profit-seeking. Accordingly, when assessing the mechanisms underlying VNSA organization learning, we must be careful to apply appropriate nuance depending on the group's aims and structure.

As this section has discussed, organizational learning is of existential importance to VNSAs. While a business that fails to innovate will see its revenue diminish, a VNSA incapable of learning will be destroyed by adversaries. The importance of learning in the VNSA context has been acknowledged by those tasked with defeating these groups, as well as the groups themselves. For example, the *U.S. Army/Marine Corps Counterinsurgency Field Manual* notes that in counterinsurgency, "the side that learns faster and adapts more rapidly—the better learning organization—usually wins."[33] Meanwhile, influential jihadist strategists Abu Musab al-Suri (born Mustafa Setmariam Nasar) and Abu Bakr Naji have both emphasized the importance of innovation and learning. As al-Suri wrote in *The Call for Global Islamic Resistance*, his 1,600-page treatise on strategy, failures on the part of jihadists were due in part to "the diffusion of yes men and decline in the levels of innovation."[34]

Despite the importance of organizational learning to VNSAs, they are still far from perfect at it. Indeed, several scholars have found militant groups to be generally conservative in their approach to innovation, and often ineffective in their efforts to learn. In a 2009 study funded by the U.S. Department of Justice's National Institute of Justice, Michael Kenney concluded that jihadists' "ability to learn is limited," in part due to "mistakes and poor tradecraft."[35] In the 2006 edition of his influential text *Inside Terrorism*, Bruce Hoffman argued that terrorists are reluctant to pursue discontinuous change because they face immense pressure to succeed at a tactical level.[36]

While these conclusions may have been entirely true at the time they were penned, we are now in a technological era that makes learning and technological change routine across various sectors, and VNSAs are no exception. We now turn to consideration of how the characteristics of VNSAs affect how these actors learn. How does a VNSA's structure, culture, ideology, strategy, and external environment affect its ability to engage in organizational learning?

Factors Influencing Organizational Learning

Given the intricacies of the process of organizational learning, it should be no surprise that a wide range of factors can influence the outcome. These include internal dynamics (organizational structure, intra-group communications, culture, membership and strategy) and external factors, such as the political and social environment in which a group operates.

Organizational Structure. The degree of centralization and bureaucratization in an organization will affect its ability to explore new knowledge, and exploit and disseminate that knowledge internally. A complex relationship exists between centralization and organizational learning. Organizations that are more decentralized are generally well equipped to engage in exploration: Cells in a decentralized

[33] *The U.S. Army/Marine Corps Counterinsurgency Field Manual* (Chicago: University of Chicago Press, 2007), p. 10.
[34] Abu Musab al-Suri, *The Call for Global Islamic Resistance* (2006), p. 859.
[35] Michael Kenney, *Organizational Learning and Islamic Militancy*, NIJ award no. 2006-IJ-CX-0025 (September 29, 2008), p. 5.
[36] Bruce Hoffman, *Inside Terrorism* 2d ed. (New York: Columbia University Press, 2006), p. 36.

structure do not have to coordinate their behavior across a hierarchy, and have more autonomy to pursue new knowledge.[37] Greater adaptability and flexibility also allow decentralized groups to respond in an agile manner as problems grow more complex. As Wharton School professors Nicolaj Siggelkow and Daniel Levinthal explain, "a key reason for decentralization is the ability to overcome the slowness of sequential decision processes."[38]

But decentralization presents obstacles to the exploitation of information. Decentralized entities have trouble sharing and absorbing knowledge internally.[39] Because decentralized organizations struggle to commit knowledge to their institutional memory, they may lose information when key learners depart (or, in the case of VNSAs, are killed or captured).[40] It is also difficult for decentralized groups to implement strategic-level changes across the organization.[41] Cells in a decentralized structure may pursue objectives independent of the broader organization's interests. In cases of extreme decentralization, disparate cells may not communicate with one another at all, thus confining organizational learning to the cellular level.[42]

Greater centralization presents its own set of benefits and challenges. Centralized organizations are often ill-suited to engage in robust exploration activities because of the amount of bureaucracy and coordination involved in decision-making. Such organizations may "plod along slowly and relentlessly."[43] Centralization is, however, conducive to the exploitation of existing knowledge. Centralization improves internal coordination, which facilitates the transmission of information throughout the organization, reduces redundancy in the exploration process, and reduces "competition and deception" between cells involved in exploration.[44] Despite this advantage, centralized organizations are not always perfectly situated for exploiting information. Information must pass through multiple layers of bureaucracy before it can be fully assimilated. Information may thus become distorted, condensed or lost, resulting in incomplete and potentially inaccurate transfers of knowledge.

Though the centralization-decentralization dichotomy offers a helpful framework for analyzing the relationship between organizational structure and learning, it does not fully capture the fluidity of many VNSAs' organizational structures. VNSAs, generally speaking, are neither fully centralized nor decentralized. They often maintain a dynamic balance between the two models.

Communication. Another key determinant of learning is an organization's capacity to communicate. The entire process of organizational learning depends on the ability to transmit information internally. Effective exploration cannot occur unless units responsible for gathering new

---

[37] For a review of the benefits associated with decentralized networks or "teams," see Kathleen Carley, "Organizational Learning and Personnel Turnover," *Organization Science* 3:1 (1992), pp. 20-46.
[38] Nicolaj Siggelkow and Daniel Levinthal, "Temporarily Divide to Conquer: Centralized, Decentralized, and Reintegrated Organizational Approaches to Exploration and Adaptation," *Organization Science* 14:6 (2003), p. 655.
[39] Calvert Jones, "Al-Qaeda's Innovative Improvisers: Learning in a Diffuse Transnational Network," *Cambridge Review of International Affairs* 19:4 (2006), p. 563.
[40] Carley, "Organizational Learning and Personnel Turnover"; Romme and Dillen, "Mapping the Landscape of Organizational Learning," pp. 66-78.
[41] Jackson et al., *Aptitude for Destruction, Vol. 1*, p. ix.
[42] Christina Fang, Jeho Lee and Melissa Schilling discuss the pitfalls associated with decentralization in "Balancing Exploration and Exploitation Through Structural Design: The Isolation of Subgroups and Organizational Learning," *Organization Science* 21:3 (2010), pp. 625-42.
[43] Carley, "Organizational Learning and Personnel Turnover."
[44] Ibid., p. 22.

knowledge are aware of the knowledge that other units and members already possess. Exploitation requires that organizations disseminate knowledge from exploratory units, both for interpretation and later for storage. If knowledge is not transmitted, or if it is distorted in the process of transmission, the learning process will be imperfect and potentially ineffective.

Jackson et al.'s study on terrorist organizational learning identified two variables that affect communications and hence learning: the type of platform used to communicate knowledge, and the degree of communication between various units within an organization.[45] The communications platform affects how different kinds of knowledge are transmitted. Explicit knowledge can be conveyed through face-to-face interactions or encoded information (*e.g.*, manuals or books). But tacit knowledge is best conveyed through experiential learning and interpersonal communication. It remains difficult for VNSAs to transmit tacit knowledge due to the security risks of congregating and training in public.

The tension between information-sharing and internal security may affect other variables relevant to VNSAs' ability to communicate knowledge. Operational security considerations may inhibit groups from sharing information internally in a timely manner. VNSA cells operating under security constraints may also seek to limit the *amount* of information they disseminate at any given time, hoping that they can reduce their exposure.

Membership of an organization. Though much organizational learning literature focuses on system-level factors, Jackson et al.'s report recognizes that the quality and makeup of an organization's personnel also has a profound effect. Three variables related to an organization's membership affect learning: congenital knowledge, stability of membership, and the ability of an organization to absorb new knowledge.

Congenital knowledge refers to the knowledge that founding members possess. Huber notes that "organizations do not begin their lives with clean slates."[46] Instead, the information an organization acquires at its conception is an aggregation of pre-existing knowledge held by the founders. This "inherited knowledge" shapes the organization's initial direction. Congenital knowledge also has a distinct impact on how new organizations learn. The characteristics, principles, and assumptions of a VNSA's founders will be instructive in anticipating important aspects of how that group will learn throughout its life cycle.

Congenital knowledge influences an organization's ability to absorb new knowledge. An organization's absorptive capacity depends on both its learning process and the kind of knowledge being absorbed. New knowledge that is similar to knowledge an organization already possesses will be easy to absorb, while it may take longer for an organization to assimilate "foreign" knowledge, or information of a kind that an organization has never seen before.[47] An organization's culture, including its willingness to assimilate knowledge that conflicts with existing assumptions, is another key determinant of absorptive capacity.

Another factor salient to determining the outcome of VNSA learning is the stability of a group's membership. High levels of attrition or personnel turnover can have a deleterious effect. But

[45] Jackson et al., *Aptitude for Destruction, Vol. 1*.
[46] Huber, "Organizational Learning," p. 91.
[47] Jackson et al., *Aptitude for Destruction*.

there is also a positive, if unintended, organizational-learning consequence to personnel turnover. "Old-timers"—people who have been with an organization for an extended time—thrive at exploitation, in large part because they are already attuned to an organization's procedures and policies. But they are often ineffective explorers, and can even be a source of inertia or resistance to new approaches.[48] Newcomers are less aware of, and less constrained by, institutional processes, making them well-equipped to engage in exploration, though not in exploitation.[49]

These findings are relevant to understanding the effect of personnel turnover on VNSAs' organizational learning. VNSAs experience disproportionately high levels of attrition, due to kill/capture operations, arrests, conflict with other groups, and defections, among other causes. Such turnover is disruptive. The elimination of highly connected individuals in compartmentalized VNSAs, for example, is likely to hamper intra-group communication and coordination, and hinder the group's efforts to exploit knowledge that it has gathered.

But high levels of personnel turnover and attrition may also drive VNSA innovation. New ideas and concepts are constantly introduced. Because personnel turnover prevents the creation of rigid hierarchies, newcomers are able to make meaningful contributions. The omnipresent risk of death provides further incentive for newcomers to innovate and overcome stagnation.

Daesh's external operations wing is one case where attrition created both challenges and also new opportunities for learning. The Amn al-Kharji, as the Islamic State's external operations wing is known internally, experienced a high rate of turnover, largely due to aggressive targeting efforts by the U.S. and other members of the anti-Daesh military coalition.[50] In light of this pressure, the Amn al-Kharji has slowed Daesh's external operations tempo. But at the same time, Daesh has continued to mount attacks across the West—many of them through its "virtual plotter" model—and has continued to find innovative means to carry out plots.

Organizational Culture and Learning Mechanisms

Osama bin Laden's early efforts to encourage al Qaeda's rank-and-file to innovate instilled an entrepreneurial spirit in that organization.[51] These efforts showcase the impact that organizational culture has on learning processes and outcomes. An organization's culture determines how it approaches learning opportunities. An organization that encourages risk-taking can inspire personnel to innovate. Conversely, an organization that prefers stability and continuity can discourage members from pursuing new learning opportunities.

---

[48] Fabrizio Perretti and Giacomo Negro, "Filling Empty Seats: How Status and Organizational Hierarchies Affect Exploration Versus Exploitation in Team Design," *Academy of Management Journal* 49:4 (2006), p. 761.
[49] Ibid.
[50] For background on the targeting of ISIS's external operatives, see W.J. Hennigan, "The U.S. Military Is Targeting Islamic State's Virtual Caliphate by Hunting and Killing Its Online Operatives One-by-One," *Los Angeles Times*, May 5, 2017; Adam Goldman & Eric Schmitt, "One by One, ISIS Social Media Experts Are Killed as Result of F.B.I. Program," *New York Times*, November 24, 2016.
[51] See Daveed Gartenstein-Ross & Nathaniel Barr, "How al-Qaeda Works: The Jihadist Group's Evolving Organizational Design," *Current Trends in Islamist Ideology*, May 30, 2018, https://www.hudson.org/research/14365-how-al-qaeda-works-the-jihadist-group-s-evolving-organizational-design; Jones, "Al-Qaeda's Innovative Improvisers"; Assaf Moghadam, "How al Qaeda Innovates," *Security Studies* 22:3 (2013), p. 466-97.

The preferences of an organization's founders and leaders heavily influence the culture that the organization adopts. Leaders play an outsize role in setting the tone for an organization, especially in its infancy. They dictate strategy, establish policies and procedures, and shape the organizational direction.

A second aspect of culture that affects organizational learning is a group's tolerance of risk.[52] In order to support and facilitate a successful learning process, organizations must be willing to tolerate risk, and even encourage personnel to make mistakes as they experiment.[53] Organizations that exhibit aversion to risk will foster an atmosphere in which members are discouraged from innovating and testing new ideas.

Some private sector firms, aware of the positive relationship between risk tolerance and innovation, have gone to considerable lengths to foster environments where employees are encouraged to experiment, and even to make mistakes. The payroll services company SurePayroll offers an annual $400 award, known as the "Best New Mistake Award," to employees who take risks and learn from their mistakes. Explaining the rationale behind the award, SurePayroll's president said, "If you don't encourage people to take risks, then you end up with incrementalism forever. Mistakes are the tuition you pay for success."[54] Dean Keith Simonton, a scholar of innovation, observed that "the most successful people tend to be those with the most failures."[55]

The factors that VNSAs consider when determining their tolerance for risk differ significantly from the factors weighed by for-profit companies. On the one hand, the cost of failure may be far greater for VNSAs, as employees of for-profit firms who make errors typically aren't killed or arrested. On the other, VNSAs must constantly adapt to the evolving challenges posed by state actors and other rivals. Thus, as these groups determine their risk tolerance, they must balance the perils of failure with the consequences of inaction and stagnation.

External Environment. In the years leading up to 9/11, al-Qaeda's base in Afghanistan served as an ideal location from which to train recruits and formulate new plots. Facing only limited pressure from counterterrorism forces, the group methodically planned 9/11 over a period of months, and deployed cells to Western Europe and the United States to lay the groundwork for the attack. By September 2001, al-Qaeda was well positioned to carry out its mission.

The preparation for the 9/11 plot illustrates how an organization's external environment can influence the way it learns. This is another point of divergence between VNSAs' organizational learning and the learning of for-profit entities. For VNSAs, the external environment can fundamentally shape how learning occurs, and even derail organizations that are well positioned internally to engage in exploration and exploitation. The external factor of paramount importance to VNSAs is the level of security in areas where they operate. Groups in a high-threat environment must often transform their structure and policies to ensure their security. And, as discussed earlier, the security measures that VNSAs implement often have a detrimental impact on learning outcomes.

---

[52] This factor is discussed in Jackson et al., *Aptitude for Destruction, Volume 1*.

[53] Laurence Weinzimer and Candace Esken, "Learning from Mistakes: How Mistake Tolerance Positively Affects Organizational Learning and Performance," *The Journal of Applied Behavioral Science*, 53:3 (2017), pp. 322-48.

[54] Leigh Buchanan, "Rethinking Employee Awards," *Inc.*, July 5, 2011.

[55] Sue Shellenbarger, "Better Ideas Through Failure," *Wall Street Journal*, September 27, 2011.

On the other hand, groups operating in a low-threat environment can engage in robust exploration and exploitation. Al-Qaeda's experience in Afghanistan before 9/11 demonstrates the possibilities for learning that are available to non-state groups in permissive locations. Al-Qaeda's training camps played a particularly crucial role. The camps hosted fighters from across the globe, and emerged as repositories of organizational memory. The camps were also vital in facilitating the transfer of implicit knowledge: Militants obtained real-world experience in operational tradecraft, and weapons and explosives training at these camps, and many later returned to their home countries to transmit their knowledge to others.[56]

With these factors influencing organizational learning in mind, this study now turns to two extended case studies describing how the technology adoption curve functions in practice, in the case of social media and the virtual plotter model, and also UAS technology.

[56] Paul Cruickshank, "Learning Terror: The Evolving Threat of Overseas Training to the West," in Magnus Ranstorp and Magnus Normark, *Understanding Terrorism Innovation and Learning: Al-Qaeda and Beyond* (New York: Routledge, 2015), loc. 3838.

Social Media and the Virtual Plotter Model

For ideological VNSAs seeking to draw others to their cause, social media serves as a megaphone of unprecedented proportions. A rich body of research produced by psychologists, sociologists, and communication scholars stretching back to even before the advent of social media helps to explain why this is so. Academics have been studying the impact of computer-mediated communication (CMC) on human behavior since the 1960s. The literature on the subject, especially three concepts from the field of social psychology—identity demarginalization, group polarization, and the social identity model of de-individuation effects—has strong explanatory power regarding the impact of the online space, particularly for VNSAs that depend on radicalizing others.

Identity demarginalization theory, as articulated by Katelyn McKenna and John Bargh in a 1998 study, explores why some social groups are more drawn to online communication than others. McKenna and Bargh found that individuals with "concealable and culturally devalued identities" were more likely to participate in and value online communities than individuals with mainstream identities.[57] Specifically, their study found that people who posted in online forums dedicated to concealable identities such as homosexuality or drug usage valued the feedback and opinions of other group members more strongly than did members of forums focused on marginalized identities that are easier to perceive, such as obesity and stuttering. "For the first time," the authors wrote, an individual exploring his or her marginalized identity in an online environment "can reap the benefits of joining a group of similar others: feeling less isolated and different, disclosing a long secret part of oneself, sharing one's own experiences and learning from those of others, and gaining emotional and motivational support."[58]

Online communities may be uniquely powerful among groups with concealable identities because the Internet provides more anonymity, reach, and in-group reinforcement than these people are likely to find in mainstream society. Relative anonymity can embolden individuals with concealable marginalized identities to discuss issues that may be taboo in a mainstream social setting.[59] For example, in a study of lesbian, gay, and bisexual (LGB) online groups, one woman noted: "I think it's much easier to talk about certain things online such as relationships, sexual things and compliments and insults. It's easier to talk to someone when you don't have to see the physical reaction and think of a response right away."[60]

In a study examining the website Stormfront and the white nationalist movement, Neil Caren et al. noted that the absence of spatial boundaries allows online communities "to draw in otherwise isolated movement participants."[61] The same phenomenon has been observed in online interactions

---

[57] Katelyn Y.A. McKenna & John Bargh, "Coming Out in the Age of the Internet: Identity 'Demarginalization' Through Virtual Group Participation," *Journal of Personality and Social Psychology* 75:3 (1998), pp. 681-94.
[58] Ibid.
[59] Neil Coulson, "Receiving Social Support Online: An Analysis of a Computer-Mediated Support Group for Individuals Living with Irritable Bowel Syndrome," *Cyberpsychology & Behavior* 8:6 (December 2005), pp. 580-84, https://www.ncbi.nlm.nih.gov/pubmed/16332169.
[60] Lynne Hillier, Kimberly J. Mitchell & Michele L. Ybarra, "The Internet as a Safety Net: Findings From a Series of Online Focus Groups with LGB and Non-LGB Young People in the United States," *Journal of LGBT Youth* 9:1 (2012), p. 225-46, http://www.unh.edu/ccrc/pdf/CV238.pdf. Here we use the relatively limited terms of *lesbian, gay, and bisexual* when characterizing sexual preferences because this was the authors' rendering for their study.
[61] Neal Caren, Kay Jowers & Sarah Gaby, "A Social Movement Online Community: Stormfront and the White Nationalist Movement," *Media, Movements, and Political Change* 33:1 (2012), pp. 163-93.

between salafi jihadists. As J.M. Berger remarked in Senate testimony: "It's different than the 1950s when, if a radical jihadist was in Peoria, he might go his whole life without finding somebody who shares his views. Now it may take 10 minutes."[62]

Participation in online communities can also reinforce what McKenna and Bargh dubbed demarginalization. Their study found that people who actively took part in online discussions not only came to "consider the group identity more important than did those who did not actively participate," but also intensified marginalized behaviors based on positive reinforcement from other group members.[63] A 2008 study of pro-anorexia online communities found that such forums were "an ideal space for maintaining and validating a pro-anorexic identity."[64] Pro-anorexia individuals participating in the forums received encouragement and guidance from like-minded members, which reinforced the forum participants' commitment to their pro-anorexia identities. Joining and receiving positive feedback from a like-minded group online can help members come to view their concealed identities more positively, sometimes to the point of incorporating them into their public personas.

The Internet's ability to help individuals reinforce and even publicly embrace once-concealed marginal identities is neither inherently good nor bad. There is obviously an enormous moral gulf between one individual coming to accept the fact that he is gay and a second person coming to positively embrace his identity as a white supremacist. The key point here is the power of online communities to cause individuals to adopt and, crucially, decide to act upon the group's violent extremist ideology.

Group polarization theory expands on some of the themes highlighted in identity demarginalization. Group polarization refers to the propensity for groups to become more extreme in their outlook through mutual reinforcement.

As with identity demarginalization, this process is neither inherently good nor bad. It can produce both virtuous and vicious cycles, but tends to magnify group cohesion either way. Numerous studies conclude that groups which interact online experience a greater degree of group polarization than groups that interact face-to-face.[65] A key reason may be the general absence of visual and verbal cues in online communication. As the LGB forum participant quoted earlier observed, people interacting online can speak freely without having to worry about the physical expressions of their peers. This reduces inhibitions, and participants become willing to "contribute more novel arguments and engage in more one-upmanship behavior," which may drive group polarization.[66]

The *social identity model of deindividuation effects (SIDE)* provides a framework for understanding processes like group polarization and demarginalization in an online setting. SIDE is a revision of classic deindividuation theory, which suggests that group immersion and anonymity within a group

---

[62] J.M. Berger, "Social Media and Terrorism," testimony before the Senate Homeland Security and Governmental Affairs Committee, May 7, 2015, https://www.c-span.org/video/?c4537154/jm-berger-remarks.
[63] Mckenna & Bargh, "Coming Out in the Age of the Internet."
[64] Jeffrey Gavin et al., "The Presentation of 'Pro-Anorexia' in Online Group Interactions," *Qualitative Health Research* 18:3 (March 2008), p. 325-33, https://www.ncbi.nlm.nih.gov/pubmed/18235156.
[65] Choon-Ling Sia et al., "Group Polarization and Computer-Mediated Communication: Effects of Communication Cues, Social Presence, and Anonymity," *Information Systems Research* 13:1 (March 2002), pp. 70-90.
[66] Ibid.

result in a loss of self-awareness and an increase in anti-normative behavior.[67] SIDE, in contrast, concludes that in an online context, anonymity and group immersion do not foster anti-normative behavior. Rather, they cause participants to ignore differences between in-group members, and to more closely embrace a group identity. As Tom Postmes et al. have explained, the SIDE model found that individuals who adopt a group identity are receptive to group cues, and are thus more susceptible to adopting the behavior of that group, regardless of whether such behavior is normative or anti-normative in society as a whole.[68]

The SIDE model has significant implications for online communications. Several studies have suggested that the Internet reduces the importance of personal characteristics and interpersonal differences, and increases the salience of group identity and group norms.[69] Anonymity in interactions may also accentuate distinctions between members of the group and non-members, and intensify intergroup hostility.

Other factors beside anonymity may also facilitate the shift from individual to group identity online. In a 2011 study, Haines et al. modified the SIDE model, concluding that group identity becomes more salient in online interactions when a group identifier (for example, avatars distinguishing in- and out-group members) is visible.[70] Haines et al. found that individuals with some (even limited) awareness of the opinions of other group members were more likely to conform to group norms than were individuals who had no awareness of other group members' opinions. Haines et al. concluded that group influence decreases in completely anonymous online situations—for example, where "no labels are attached to comments"—due to lack of awareness of others' opinions. But group influence increases when common group identifiers exist. This finding is particularly relevant for platforms like Twitter and Facebook, where group identifiers can be reflected in avatars and other symbols attached to a user's profile.

Identity demarginalization, group polarization and SIDE all have considerable explanatory power in explaining online radicalization. All three theories demonstrate that certain characteristics of online communications, including reduced social cues and anonymity, often strengthen group influence at the expense of individual identity. Group polarization and identity demarginalization explain the social mechanisms by which political extremism and other fringe identities can become validated and more pronounced in online communications.

Extremist VNSAs recognize the value of the online space. Social media affords them a unique level of peer-to-peer interaction between like-minded individuals, irrespective of their proximity to each other. Those with criminal or extremist interests may have previously struggled to find communities of individuals who shared these interests, but those communities, and their members, are increasingly accessible through social media. Community members often establish personal relationships and a sense of what Berger calls "remote intimacy."

---

[67] Philip Zimbardo, "The Human Choice: Individuation, Reason, and Order Versus Deindividuation, Impulse, and Chaos," *Nebraska Symposium on Motivation* 1:17 (1969), pp. 237-307, https://psycnet.apa.org/record/1971-08069-001.

[68] Tom Postmes et al., "Breaching or Building Social Boundaries? SIDE-Effects of Computer-Mediated Communication," *Communication Research* 25:6 (1998).

[69] Tom Postmes et al., "Social Influence in Computer-Mediated Communication: The Effects of Anonymity in Group Behavior," *Personality and Social Psychology Bulletin* 27:10 (October 2001), https://journals.sagepub.com/doi/abs/10.1177/01461672012710001.

[70] Russell Haines et al., "A New Perspective on De-Individuation via Computer-Mediated Communication," *European Journal of Information Systems* 20:2 (March 2011), p. 156-67, https://link.springer.com/article/10.1057%2Fejis.2010.70.

To date, no VNSA has harnessed social media as effectively as Daesh, though its effectiveness has recently declined as its social media efforts moved into the *competition* phase on the technology adoption curve. As one example of its proficiency during the group's peak, over 46,000 Twitter accounts were operated by the group's supporters from September to December 2014. With an average of 1,000 followers per account, Daesh was able to broadcast content to millions of people across the globe on Twitter alone.[71] In part due to the strength of Daesh's online communications, nearly 42,000 foreign fighters, hailing from over 120 countries, were drawn to fight with militant groups in Iraq and Syria.[72] These fighters provided Daesh with unprecedented levels of manpower, eclipsing the number of fighters who joined the mujahedin in 1980s-era Afghanistan and the al-Qaeda insurgency in mid-2000s Iraq.[73] The group also tailored its social media recruitment toward specific skill sets, such as doctors, computer programmers or media operatives.

In addition to bolstering its caliphate, social media was integral to Daesh's revolutionary virtual plotter model. In this model, operatives who are part of Daesh's external operations division plot attacks online with supporters across the globe. The plotters provide logistical, tactical, and sometimes even emotional support to sympathizers seeking to carry out attacks. Whereas this level of interaction between plotter and operative used to be reserved for face-to-face meetings, most of the supporters who tried to carry out attacks never personally meet the Daesh operatives with whom they are conspiring.

Daesh's successful adoption of the virtual plotter model was neither instantaneous nor spontaneous. It built upon earlier groups' attempts, and was facilitated in large part by consumer-side improvements to social media platforms and burgeoning populations of social media users. We begin this section by examining jihadists' *early adoption* of social media, focusing in particular on Anwar al-Awlaki. We then turn to Daesh's *iteration* on earlier attempts to inspire external operations through social media. Then we describe Daesh's *breakthrough*, where the group began to harness social media and encrypted communication platforms to have more consistent success in launching virtually plotted attacks. Finally, we discuss the ongoing *competition* phase, which highlights the countermeasures put in place by social media companies and governments to mitigate Daesh's virtual plotter model.

Early Adoption: Anwar al-Awlaki

---

[71] J.M. Berger & Jonathon Morgan, *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter* (Washington, DC: The Brookings Institution, March 2015), https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.

[72] Joana Cook & Gina Vale, *From Daesh to 'Diaspora': Tracing the Women and Minors of the Islamic State* (London: International Centre for the Study of Radicalisation, July 2018), https://icsr.info/wp-content/uploads/2018/07/Women-in-ISIS-report_20180719_web.pdf.

[73] Estimates of the number of foreign fighters in 1980s Afghanistan vary from 10,000 to 35,000, while estimates of the number of foreign fighters in mid-2000s Iraq vary from 4,000 to 5,000. See Peter Bergen, *The Osama bin Laden I Know: An Oral History of al-Qaeda's Leader* (Washington, DC: Free Press, 2006); Ahmed Rashid, *Taliban: Militant Islam, Oil and Fundamentalism in Central Asia* (New Haven, CT: Yale University Press, 2010); Thomas Hegghammer, "The Rise of Muslim Foreign Fighters," *International Security* 35:3 (Winter 2010/11), p. 61, https://www.belfercenter.org/sites/default/files/legacy/files/The_Rise_of_Muslim_Foreign_Fighters.pdf.

Prior to Daesh, al-Qaeda was a pioneer in its use of social media not only to propagandize, but also to inspire attacks beyond core territory where it operated.[74] Al-Qaeda's most prominent social media innovator, Anwar al-Awlaki, was also among its most prolific external operations planners.

Before he became a globally infamous al-Qaeda propagandist and high-level leader of al-Qaeda in the Arabian Peninsula (AQAP), Awlaki lived in the United States. He served as the imam of a mosque in San Diego from 1996 to 2000, then as an imam at the Dar al-Hijrah Mosque in Falls Church, Virginia from 2001 to 2002.[75] His background and credentials as a cleric would later add to his credibility in the eyes of his target audience. During this period, Awlaki was media savvy, and sometimes was referred to as a moderate in the press. In November 2001, for example, the *Washington Post* featured Awlaki in an online Q&A explaining the Ramadan fast.

In 2002, Awlaki left the United States, possibly because he feared that a FBI investigation into his solicitation of prostitutes would become public, and moved to London. In the following years, Awlaki grew increasingly publicly critical of the United States and the West. In 2004, he relocated permanently to Yemen. The same year, Awlaki was arrested by Yemeni security services and detained for around 18 months. Upon his release, Awlaki moved to the remote province of Shabwah in eastern Yemen, where he became known as an AQAP spokesman and official.

Awlaki's fluency in English and Arabic, as well as his calm and measured delivery, appear to have been key to his charisma. According to a 2011 report by Alexander Meleagrou-Hitchens, Awlaki's historical knowledge added to his resonance. Meleagrou-Hitchens notes that "Awlaki's ability to juxtapose key moments from the early history of Islam onto the present situation of Western Muslims made him immensely popular and easily accessible."[76]

Awlaki became highly influential due in part to his effective early adoption of social media platforms. Awlaki posted many of his sermons to YouTube, in addition to keeping a blog. Religious novices and hardened jihadists alike could suddenly access an authoritative extremist cleric from the comfort of their own homes. In the wake of the 2009 Fort Hood shooting, in which U.S. Army psychiatrist Nidal Hassan murdered 13 people and wounded 31 others, Awlaki authored a post titled "Nidal Hassan Did the Right Thing."

Prior to his death in a U.S. drone strike, Awlaki became notorious for using the Internet to call for "lone wolf" terrorist attacks. He hoped that lone attackers would complement rather than replace al-Qaeda's centrally directed plots—some of which, most notably Umar Farouk Abdulmutallab's Christmas Day 2009 underwear bomb plot, Awlaki himself helped to plan.[77] Through

---

[74] Though al-Qaeda's use of the Internet to propagandize and engage with supporters stretches back to before the social media era, we begin our discussion with Awlaki's social media-based efforts. They form the clearest parallel to Daesh's current use of social media. For further discussion of al-Qaeda's early use of the Internet, see Bruce Hoffman, "The Use of the Internet by Islamic Extremists," testimony presented to the House Permanent Select Committee on Intelligence, May 4, 2006, https://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT262-1.pdf.

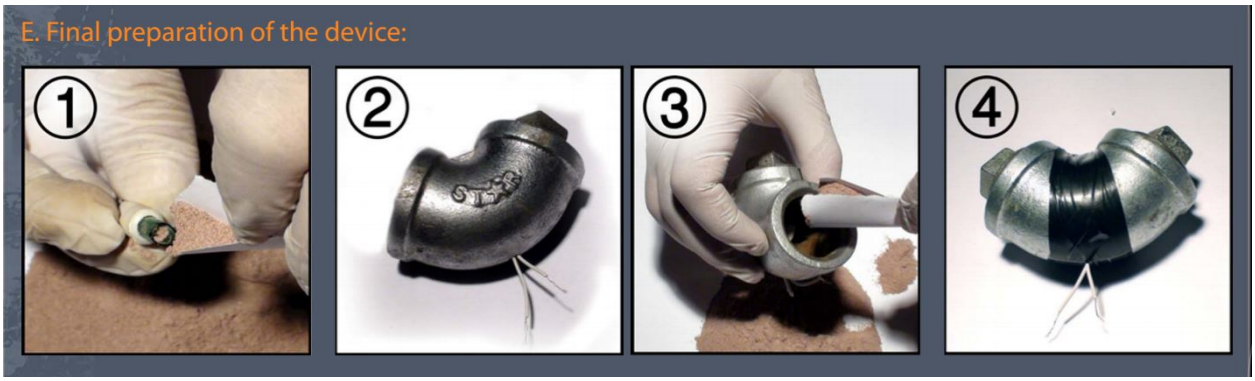
[75] Joseph Rhee & Mark Schone, "How Anwar Awlaki Got Away," *ABC News*, November 30, 2009, https://abcnews.go.com/Blotter/FtHoodInvestigation/anwar-awlaki/story?id=9200720.

[76] Alexander Meleagrou-Hitchens, *As American as Apple Pie: How Anwar al-Awlaki Became the Face of Western Jihad* (London: The International Centre for the Study of Radicalisation and Political Violence, 2011).

[77] See Peter Finn, "Al-Awlaki Directed Christmas 'Underwear Bomber' Plot, Justice Department Memo Says," *The Washington Post*, February 10, 2012 (noting that Awlaki "personally directed" Abdulmutallab's plot, according to a Department of Justice memo).

his public statements, particularly his YouTube sermons, Awlaki mobilized a large number of people. According to the Counter Extremism Project research organization, Awlaki's videos and writings influenced around 90 known extremists in the United States and Europe as of 2017, some even after his death.[78] Plots influenced, at least in part, by Awlaki include the April 2013 Boston Marathon bombings, December 2015 San Bernardino attack, June 2016 shooting at the Pulse nightclub in Orlando, and the September 2016 bombings in New York and New Jersey.[79]

Awlaki's calls for his followers to take up arms resonated with many. AQAP provided further fuel through its web-based English-language *Inspire* magazine. Published by Awlaki and Samir Khan, another American AQAP member, *Inspire* included propaganda, updates on the group's activities, and interviews with prominent jihadists. Each issue also included a section called "Open Source Jihad," described by the publication as "a resource manual for those who loathe the tyrants; includes bomb making techniques, security measures, guerrilla tactics, weapons training, and all other jihadi activities."[80] Articles published in this section had titles that included "Designing a Timed Hand Grenade," "Qualities of an Urban Assassin," and "The Hidden Bomb." Each of these articles included detailed instructions on how to build a weapon or implement a tactic. The authors also included pictures and diagrams to supplement their written instructions.



Above: One of the diagrams included in the Inspire *article "How to make a bomb in the kitchen of your mom"*

Inspire was not social media. Yet though it did not provide the same level and style of guidance as Daesh's virtual plotters later would, "Open Source Jihad" was deadly in its own right. The bomb used in the aforementioned 2013 Boston Marathon bombing was based on the design provided in the 2010 *Inspire* article "How to make a bomb in the kitchen of your mom."[81]

Awlaki's successful use of YouTube to radicalize people to carry out violent attacks showed the immense promise of social media even during the early adoption phase. Yet Awlaki could not match the pace of mobilization that later virtual plotters would obtain. Though YouTube is a social media platform, Awlaki employed it more like a Web 2.0-style blog, rather than fostering remote

---

[78] Counter Extremism Project, *Anwar al-Awlaki* (n.d.), https://www.counterextremism.com/sites/default/themes/bricktheme/pdfs/Anwar_al-Awlaki_Ties.pdf.

[79] See discussion in Scott Shane, et al., "'In-Betweeners' Are Part of a Rich Recruiting Pool for Jihadists," *The New York Times*, September 23, 2016.

[80] "Open Source Jihad," *Inspire*, Issue 1, January 2010, p. 32, https://azelin.files.wordpress.com/2010/06/aqap-inspire-magazine-volume-1-uncorrupted.pdf.

[81] Azmat Khan, "The Magazine that 'Inspired' the Boston Bombers," *Frontline*, April 30, 2013, https://www.pbs.org/wgbh/frontline/article/the-magazine-that-inspired-the-boston-bombers/.

intimacy through constant interaction with potential operatives. (We explain the distinction between Web 2.0 and the Social Web in the following section.) Further, though Awlaki was effective at radicalizing people and spurring them on to action, he was unable to devise a way to fold attackers into al-Qaeda's overarching strategy. In other words, he put out *general* calls for action which were heeded at an alarming rate, but he did not *specifically* follow up with attackers to make sure their efforts were maximally effective or interwoven into al-Qaeda's global strategy. Accordingly, he sowed chaos and fear, but the early adoption phase provided only a small taste of what was yet to come.

Iteration

Daesh's stunning success on social media should be understood in the context of the group's ability to capture the public imagination even beyond the social media realm. Daesh's newest spate of atrocities in Iraq and Syria made headlines and dominated cable news practically every night. Social media helped the group powerfully capitalize on this dynamic.

Technological Improvements. Social media platforms did not drastically evolve between the period of Awlaki's prominence and the rise of Daesh's virtual plotters. But three distinct changes occurred. First, the unique capabilities of social media became better understood, and the practices of engaging followers on social media became increasingly distinct from those employed in the Web 2.0 world. Second, far more people worldwide were drawn to social media. Third, advances in encryption allowed secure conversations between jihadist influencers and operatives that would likely have resulted in arrests during Awlaki's prime.

Turning to the Web's evolution, the Internet as it exists today is a far cry from where it stood in the 1990s. The first iteration of the Internet, Web 1.0—the "read-only" Web—was characterized by static webpages that could be read but offered little to no interactivity. Around the turn of the century, Web 2.0, or the "read-write" Web, emerged. This iteration allowed users to create blogs, post multimedia content (*e.g.*, audio recordings or videos), and engage more easily with content on webpages. Web 2.0 offered greater interactivity but did not change the average Web user into a content producer.

The social web turned this dynamic on its head. On sites in the social web—including Facebook, MySpace, Twitter, and YouTube—users were no longer primarily consumers of someone else's material, but were put into the position of being content producers themselves.[82] Awlaki rose to prominence just as Web 2.0 was giving way to the social web. But he used the social web largely the same way that content producers used Web 2.0: His content was far and away the primary message, and interactivity with his audience was at best of secondary concern. Techniques for gathering a loyal and devoted audience, and for cultivating personal relationships via the social web that seemed deep and meaningful, became further refined after Awlaki's death. Daesh emerged in the context of this deeper realization of the social web's potential not only for entertainment entrepreneurs like Taylor Swift or Justin Bieber, but also for social entrepreneurs like Daesh. Daesh's use of the social web was genuinely innovative; but the group also benefited heavily by traveling paths that others had already blazed, in part because its so many of its young devotees were highly familiar with the milieu of social media.

[82] For discussion of the Internet's evolution, from Web 1.0 to Web 2.0 and then to the social web, see Eric Schmidt & Jonathan Rosenberg, *How Google Works* (New York: Hachette, 2014), locs. 3235-46.

The second major change from the early adoption to iteration phase is that, as we noted, between 2010 and 2014 the number of social media users grew sharply. For example, Facebook had 608 million monthly users at the end of 2010. By the end of 2014, that number had soared to nearly 1.4 billion.[83] Over the same time period, Twitter's user base increased from 54 million to 288 million.[84] This meant that the potential reach of Daesh propaganda vastly surpassed that of Awlaki's YouTube videos.

The third change was significant improvement in secure user-to-user communication. These improvements occurred primarily in response to former National Security Agency contractor Edward Snowden's 2013 revelations about U.S. government surveillance programs. Alarmed by the this far-reaching surveillance, many tech companies swiftly moved to improve information privacy. Foremost among these improvements was the widespread diffusion of end-to-end encryption (E2EE) technologies. The website of an email service providing E2EE communications provides a competent explanation of what makes this method of secure communication unique:

> When you use E2EE to send an email or a message to someone, no one monitoring the network can see the content of your message — not hackers, not the government, and not even the company … that facilitates your communication.
>
> This differs from the encryption that most companies already use, which only protects the data in transit between your device and the company's servers. For example, when you send and receive an email using a service that does not provide E2EE, such as Gmail or Hotmail, the company has the ability to access the content of your messages because they also hold the encryption keys. **E2EE eliminates this possibility because the service provider does not actually possess the decryption key.** Because of this, E2EE is much stronger than standard encryption.[85]

Though E2EE can be compromised by an individual posing as the intended recipient, the data itself is essentially impossible to decrypt without the proper key.[86] While E2EE was used by a relatively small number of people prior to the Snowden revelations, it spread quickly thereafter. WhatsApp, a messaging platform that now boasts over 1.5 billion users, was among the first popular platforms to adopt E2EE in November 2014.[87] Snapchat has introduced E2EE; and there are even plans underway to incorporate E2EE into Facebook Messenger, which has long been considered an insecure platform due to the company's tendency to actively surveil its users.[88] This technology once reserved for a small number of users who placed a high value on data privacy has quickly become an industry standard.

---

[83] Statista, "Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2018 (in Millions)," 2019, https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

[84] Statista, "Number of Monthly Active Twitter Users Worldwide from 1st Quarter 2010 to 4th Quarter 2018 (millions)," February 2019, https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/.

[85] ProtonMail, "What is End-to-End Encryption and How Does It Work?," March 7, 2018, https://protonmail.com/blog/what-is-end-to-end-encryption/.

[86] See, e.g., discussion in Nadeem Unuth, "What is End-to-End Encryption?" *LifeWire*, March 8, 2019, https://www.lifewire.com/what-is-end-to-end-encryption-4028873.

[87] Andy Greenberg, "WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users," *Wired*, November 18, 2014, https://www.wired.com/2014/11/whatsapp-encrypted-messaging/.

[88] See James Titcomb, "Snapchat Adds End-to-End Encryption to Protect Users' Messages," *The Telegraph* (London), January 10, 2019, https://www.telegraph.co.uk/technology/2019/01/09/snapchat-adds-end-to-end-encryption-protect-users-messages/; Mike Isaac, "Zuckerberg Plans to Integrate WhatsApp, Instagram, and Facebook Messenger," *The New*

Daesh was quick to embrace the use of E2EE platforms. The group's embrace of E2EE is not the first time that jihadists explored encryption. In the first issue of *Inspire*, AQAP provided a tutorial on how to use its own encrypted communication platform, Asrar al-Mujahideen 2.0.[89] The difference between al-Qaeda's early experimentation with encryption and Daesh's more robust and successful adoption is that the former had to rely on its own technological know-how, while Daesh could ride the wave of companies that devoted significant resources to E2EE. Indeed, our review of the Asrar al-Mujahideen 2.0 tutorial suggests that the software was clunky and difficult to use. For example, it required users to manually input their encryption keys, and was not readily accessible to those who did not actively search for it.

Daesh's Highly Structured External Operations. In describing Daesh's external operations division, this section focuses on its form and function at the time that Daesh was able to successfully implement the virtual planner model of attacks. It does not attempt to trace subsequent developments or organizational adaptations following Daesh's loss of the territory it once held. It is important to understand the structure of the group's external operations efforts at that time because organizational dynamics undeniably played a role in Daesh's implementation of the virtual plotter model. The group's robust, highly structured external operations division proved well-equipped to seize on evolving communication technologies to revolutionize its external operations methods. This external operations infrastructure has demonstrated an unprecedented ability to coordinate sustained campaigns in various theaters across the globe.

The Amniyat al-Kharji, Daesh's external operations division, was a hierarchical structure within Daesh charged with selecting and training external operatives, as well as conducting terrorist attacks outside what was the group's core territory.[90] Responsibility within the Amniyat was divided by geographic location, with operatives who can be described as theater commanders taking charge of operations extending from Europe to Southeast Asia. These theater commanders were assigned according to their nationality and linguistic capabilities, and were tasked with planning attacks in those areas.[91] Virtual plotters were integrated into this geographic command structure, where they functioned much like theater commanders, but in the cyber realm. Daesh's virtual plotters were likewise assigned areas of responsibility according to their nationality, cultural knowledge, and linguistic skills, and tasked with recruiting and handling attackers from these areas.

Early Virtual Plotters. In contrast to Awlaki's general calls for attacks, Daesh engineered a process by which its top operatives could directly guide lone attackers, playing an intimate role in the conceptualization, target selection, timing, and execution of attacks. Virtual plotters could offer operatives the same services once provided by physical networks. The model thus helped transform

---

York Times, January 25, 2019, https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html.

[89] Asrar al-Mujahideen 2.0 was released in 2008, one year after al-Qaeda released its first encrypted communication platform, Asrar al-Mujahideen. See Terr0r1st, "How to Use Asrar al-Mujahideen," *Inspire*, Issue 1, January 2010, pp. 41-44, https://azelin.files.wordpress.com/2010/06/aqap-inspire-magazine-volume-1-uncorrupted.pdf.

[90] Rukmini Callimachi, "How a Secretive Branch of ISIS Built a Global Network of Killers," *The New York Times*, https://www.nytimes.com/2016/08/04/world/middleeast/isis-german-recruit-interview.html?_r=0.

[91] Bridget Moreng, "ISIS' Virtual Puppeteers," *Foreign Affairs*, September 21, 2016, https://www.foreignaffairs.com/articles/2016-09-21/isis-virtual-puppeteers.

lone attackers who relied heavily on the Internet from the bungling wannabes they once were into something more dangerous.[92]

The experience of the first Daesh virtual plotter to gain international recognition, British hacker-turned-terrorist Junaid Hussain, to a large extent illustrates how the virtual plotter model represented an improvement over earlier Internet-based calls for attacks. Hussain maintained simultaneous involvement in several plots, including the following:

May 2015

- Hussain encouraged Elton Simpson and Nadir Soofi to attack the "Jihad Watch Muhammad Art Exhibit and Cartoon Contest" held in Garland, Texas. Simpson and Soofi arrived at the venue and opened fire, but they were quickly killed by an alert security officer.[93]

- Hussain was in contact with Munir Abdulkader, a 22-year old from West Chester, Ohio. He encouraged Abdulkader to launch an attack against U.S. military and law enforcement personnel. Authorities arrested Abdulkader after he purchased an AK-47 to further this plot.[94]

- A 17-year old with links to Hussain was arrested in Melbourne, Australia for plotting a Mother's Day massacre. Hussain provided the teen with bombmaking instructions and encouraged him to launch an attack in Melbourne.[95]

June 2015

- Hussain communicated with Usaamah Abdullah Rahim, a Daesh sympathizer who was killed while attacking a police officer and FBI agent in Roslindale, Massachusetts. An investigation following the attempted attack revealed that Hussain initially encouraged Rahim and two co-conspirators to attack Pamela Geller, who had organized the Garland art contest.[96]

- Justin Nojan Sullivan, a 19-year old from Morganton, North Carolina, conspired with Hussain to plan a mass shooting that would be claimed in Daesh's name. Sullivan was caught by the FBI before he could carry out the attack. But in the weeks before the attack, Sullivan succeeded in murdering his neighbor.[97]

---

[92] For a discussion of early lone plotters' failures, see Emily Hunt, "Virtual Incompetence," *The Weekly Standard*, August 17, 2006.

[93] Scott Shane, "Texas Attacker Left Trail of Extremist Ideas on Twitter," *The New York Times*, May 5, 2015, https://www.nytimes.com/2015/05/06/world/middleeast/isis-texas-muhammad-cartoons.html.

[94] United States Department of Justice, press release, "Ohio Man Sentenced to 20 Years in Prison for Plot to Attack U.S. Government Officers," November 23, 2016, https://www.justice.gov/opa/pr/ohio-man-sentenced-20-years-prison-plot-attack-us-government-officers.

[95] Chip Le Grand, "Seven Years for Terror Teen's Melbourne Bomb Plot," *The Australian* (Australia), December 7, 2016.

[96] U.S. Department of Justice, press release, "Two Individuals Charged in Superseding Indictment with Conspiring to Commit Acts of Terrorism Transcending National Boundaries," April 21, 2016, https://www.justice.gov/opa/pr/two-individuals-charged-superseding-indictment-conspiring-commit-acts-terrorism-transcending; Del Quentin Wilber, "Here's How the FBI Tracked Down a Tech-Savvy Terrorist Recruiter for the Islamic State," *L.A. Times*, April 13, 2017, https://www.latimes.com/politics/la-fg-islamic-state-recruiter-20170406-story.html.

[97] "Factual Basis," *United States v. Sullivan*, 1:16-cr-05-MR-DLH (W.D. N.C., November 14, 2016), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Sullivan%20Factual%20Basis.pdf.

- Hussain communicated with Fareed Mumuni and Munther Omar Saleh, members of a small Daesh cell in New York and New Jersey. Hussain encouraged Saleh to conduct a suicide bombing against law enforcement officers, and Mumuni stabbed an FBI agent who was executing a search warrant at his residence.[98]

- Hussain recruited Ardit Ferizi, a Daesh sympathizer living in Malaysia, to hack into the server for an Illinois company and release personally identifiable information on around 1,300 U.S. military or government personnel who had shopped there. Daesh subsequently released this information on Twitter as a list of targets for militants living in the United States.[99]

July 2015

- Hussain conspired with Junead Khan, who intended to attack U.S. military personnel in Britain. Hussain gave Khan bombmaking instructions and tactical suggestions. Khan was arrested prior to carrying out his attack.[100]

August 2015

- Zunaid Hussain, a doorman in Birmingham (U.K.), planned to detonate a bomb along the train tracks of a rail line between Birmingham and London. Hussain reportedly communicated with Junaid Hussain over Twitter and Kik, another messaging platform.

One case which demonstrates Hussain's capacity to serve as both a handler and friend to his operatives is that of Justin Nojan Sullivan. As noted above, Sullivan was arrested in North Carolina in June 2015. He received a life sentence for plotting his intended terrorist attack. Released excerpts of Hussain and Sullivan's chats highlight the relationship between virtual plotter and operative. Rather than solely receiving one-way directives from Hussain, Sullivan was constantly communicating with the virtual plotter, sharing his excitement about the carnage that he expected to inflict. At one point, he wrote to Hussain: "Akhi I have good news… very soon carrying out the 1st operation of Islamic State in North America." Hussain acknowledged Sullivan's excitement in one message, then in the next re-focused on the task at hand, asking Sullivan to make a martyrdom video.[101]

Another case that subtly demonstrates the advances made by the virtual plotter model is the Junead Khan plot, which was disrupted in July 2015. Khan had been on British authorities' radar since 2014, originally arousing suspicion for his desire to travel to the caliphate. In early 2015, he changed his mind and began focusing on carrying out a domestic attack, using his job as a deliveryman to scope out U.S. military bases. In July 2015, Khan and Junaid Hussain discussed the logistics of various possible plans of attack. At one point, Hussain told Khan: "Most soldiers live in bases which are

---

[98] United States Department of Justice, press release, "New York Man Sentenced to 17 Years in Prison for Attempted Murder of a Federal Officer," April 26, 2018, https://www.justice.gov/opa/pr/new-york-man-sentenced-17-years-prison-attempted-murder-federal-officer.

[99] Sentencing Memorandum, *United States v. Ferizi*, 1:16-cr-042 (E.D. Va., September 23, 2016), https://www.justice.gov/opa/file/896326/download.

[100] "U.S. Airmen Terror Attack: Junead Khan Found Guilty," *BBC* (UK), April 1, 2016, https://www.bbc.com/news/uk-35944661.

[101] Chat transcript released in "Factual Basis," *United States v. Sullivan*, 1:16-cr-05-MR-DLH (W.D. N.C., November 14, 2016), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Sullivan%20Factual%20Basis.pdf.

protected. I suppose on the road is the best idea."[102] Hussain later sent Khan a bombmaking manual, and told him to employ explosives against police who arrived on the scene of his attack.[103] While Khan may have previously been limited to passively reading about tactics and weapons in *Inspire*, the virtual plotter model allowed Hussain to workshop Khan's attack plans with him and provide tailored tactical insights.

It is worth noting the frequency with which Junaid Hussain's operatives were arrested. Indeed, from this perspective Hussain could be viewed as a failure. One critical error was the frequency with which Hussain engaged with would-be operatives through Twitter direct messages or other non-secure means of communication. While Twitter was an efficient way to find potential operatives, a single message exchanged between Hussain and another Twitter user could catch authorities' attention.[104] Another key error is Hussain's apparent failure to ensure that his operatives fastidiously deleted incriminating messages from their devices. This allowed authorities to lift key evidence from the operatives' electronic devices after taking them into custody.

But from another perspective, Hussain was not a failure, but a stunning success. While his operational security was lacking, he was able to mobilize operatives at what can described as an unprecedented pace—and this despite the fact that he lacked Awlaki's charisma and religious credentials. Such is the power of the remote intimacy that social media can foster. When future Daesh operatives were able to combine the mobilization power of social media with better operational security, the organization would reach its breakthrough phase.

Breakthrough

Junaid Hussain may have gotten his operatives arrested far more often than Daesh would have preferred, but his efforts nonetheless served as a strong proof of concept for the virtual plotter model. One change that was integral to the *breakthrough* phase was the preference Daesh developed for employing secure messaging platforms for the full duration of a virtual plotter's relationship with the operatives he was directing.

One significant adaptation was Daesh's growing use of Telegram, a secure messaging system that prides itself on data privacy.[105] Telegram included group chat and channel functions in addition to private chats.[106] Similar to Twitter's multiplicity of functions, Daesh could broadcast propaganda and communicate one-on-one with its supporters, all within the Telegram ecosystem. But unlike Twitter, the one-on-one chats between plotters and would-be operatives on Telegram could be end-

---

[102] "Luton Delivery Driver Guilty of Planning Terror Attack on U.S. Troops in Britain," *The Guardian* (London), April 1, 2016, https://www.theguardian.com/uk-news/2016/apr/01/luton-delivery-driver-junead-khan-guilty-planning-terror-attack-us-troops.

[103] "U.S. Airmen Terror Attack: Junead Khan Found Guilty," *BBC* (UK), April 1, 2016, https://www.bbc.com/news/uk-35944661.

[104] This is true despite that fact that Hussain routinely moved these conversations to end-to-end encrypted platforms. This initial Twitter connection was often reason enough for authorities to leverage other surveillance methods (*e.g.*, physical surveillance or confidential informants) against suspects. See Wilber, "Here's How the FBI Tracked Down a Tech-Savvy Terrorist Recruiter."

[105] Though Telegram is privacy-oriented, its chats are not end-to-end encrypted by default. Rather, the app requires users to actively enter into "secret chats" in order to use end-to-end encryption. See "Telegram FAQ," n.d., https://telegram.org/faq#q-what-are-your-thoughts-on-internet-privacy.

[106] Telegram group chats are invitation-only, and can support up to 200,000 members. Telegram channels can be joined by anyone and do not have a member limit.

to-end encrypted from the outset. This hindered authorities' ability to identify which individuals transitioned from group engagement to direct engagement with virtual plotters, in turn hindering the use of alternative surveillance techniques that proved effective in interdicting Junaid Hussain's would-be operatives. Telegram subsequently played a role in a number of plots, both virtual and otherwise.[107]

Two attacks that are emblematic of these improvements in operational security occurred in Germany in July 2016. The first occurred on July 18, when Riaz Khan carried out a knife attack on a train. The second came less than a week later, on July 24, when Mohammed Daleel detonated a bomb by a wine bar near a music festival. Though these attacks were small in impact—the only fatality was Daleel himself, with around 20 people wounded—they can be classified as successful insofar as authorities had no advance warning of the plots or their perpetrators.

Daleel was in direct contact with a Daesh virtual plotter throughout the planning stages of his attack, up until the moment of execution. In fact, absent Daleel's ongoing discussions with his handler, the attack may never have happened. As he scouted the target in the days prior to his attack, Daleel sent a picture to his handler, informing him that "this place will be crowded." Enthused, his handler replied: "Kill them all, so they'll be lying on the ground."[108]

As the day to attack arrived, however, Daleel was a bundle of nerves. The virtual plotter with whom he conversed helped him to overcome his doubts and redirect his attack:

> *Daleel*: "The party will be over soon, and there are checks at the entrance."
>
> *Virtual Plotter*: "Look for a suitable place and try to disappear into the crowd. Break through police cordons, run, and do it."
>
> *Daleel*: "Pray for me. You do not know what is happening with me right now."
>
> *Virtual Plotter*: "Forget the festival and go over to the restaurant. Hey man, what is going on with you? Even if just two people were killed, I would do it. Trust in God and walk straight up to the restaurant."[109]

And that is precisely what Daleel did. Heeding his handler's advice, Daleel detonated his bomb at a wine bar outside the concert, so that he didn't have to face the security barriers that he found daunting. The detonation killed Daleel and wounded 15 victims, four seriously.[110] While an operative who was truly on his own, and not in touch with a virtual plotter, may have simply aborted the attack, Daleel continued. His nerves were calmed in real-time by his handler.

Riaz Khan's experience closely mirrored Daleel's, though Khan's resolve appears to have been steeled from the outset. When Khan first indicated to his handler that he intended to carry out a knife

---

[107] Such attacks included the November 2015 Paris attacks and the January 2017 attack on the Reina nightclub in Istanbul. Abdulkadir Selvi, "Reina Terrorist's Second Target was Cumhuriyet," *Hurriyet Daily News Online* (Turkey), January 30, 2017.
[108] Transcripts of Daleel's conversations with his handler can be found in "Auch der Attentäter von Ansbach Wurde vom IS per Chat Gestuert," *Süddeutsche Zeitung* (Germany), September 14, 2016, https://www.sueddeutsche.de/politik/terror-die-chats-der-attentaeter-von-wuerzburg-und-ansbach-mit-dem-is-1.3161419-2.
[109] Ibid.
[110] Frederik Pleitgen, Tim Hume & Euan McKirdy, "Suicide Bomber in Germany Pledged Allegiance to ISIS Leader," CNN, July 26, 2016, https://www.cnn.com/2016/07/24/world/ansbach-germany-blast/index.html.

attack, the handler replied: "Brother, don't you think doing it with a car would be better?"[111] He reasoned that "the damage would be considerably bigger." Khan demurred, lamenting that he didn't "know how to drive a car." Asked why he couldn't just learn how to drive, Khan replied that he wanted "to go to paradise tonight."

Sometime after, Khan asked his handler to "pray for me to become a martyr," and updated him on his whereabouts in real time: "I'm waiting for the train." Later: "I'm about to start."[112] Though Khan opted against using a car, his plotter's suggestion may have been an important foreshadowing of the rise in vehicular attacks that later plagued Europe.

As Khan and Daleel's communications with their handlers demonstrate, the timing and logistics of their attacks—and in Daleel's case, the fact that the attacker did not back out at the eleventh hour—were directly influenced by their virtual plotters.[113] The key difference from Junaid Hussain's failed plots appears to be technological: the attackers were shielded by E2EEE throughout their engagement with Daesh. This ensured that German authorities were unable to identify the operatives in advance and interdict their attacks.[114]

Rachid Kassim. The success of Rachid Kassim, a Francophone virtual plotter who worked in Europe, may be the best demonstration of the group's *breakthrough* with the virtual plotter model. Kassim, a French social worker turned jihadist, travelled to Syria to join Daesh in 2015. Like Junaid Hussain, he established a noteworthy social media presence, using his ability to speak both French and Arabic to connect with aspiring jihadists in his home country.[115] Kassim ran a popular Telegram channel, Sabre de Lumière (Sword of Light), in which he called for attacks in European countries and distributed "hit lists" of high-profile individuals.[116] He also engaged one-on-one with aspiring operatives, assisting them in carrying out attacks. Prior to his death in a July 2017 U.S. airstrike, Kassim was involved in a number of plots, including the following:

June 2016

- French authorities believe Kassim was in contact with Larossi Abballa, a 25-year-old French jihadist who murdered a police captain and his partner in Magnanville, France.[117] After slaying the couple, Abballa menaced their three-year-old child. He streamed the abuse on Facebook

---

[111] The chat transcripts can be found in Hans Leyendecker & Georg Mascolo, "Germany's 'Remote-Control' Terror Attacks, Online Chats Revealed," *Suddeutsche Zeitung* (Germany), September 21, 2016, https://www.worldcrunch.com/terror-in-europe-1/germanyas-quotremote-controlquot-terror-attacks-online-chats-revealed.

[112] Ibid.

[113] It is unclear whether the virtual plotter was the same in both attacks. Given Daesh's theater-based command structure, both men may have had the same virtual plotter.

[114] See discussion in Simon Shuster, "Why Germany Doesn't Know The Identity of its ISIS Attacker," *Time*, July 20, 2016, http://time.com/4415501/germany-isis-ax-train-attack-terrorism/; Melissa Eddy & Boryana Dzhambazova, "How a Suicide Bomber Made His Way From Syria to Strike in Ansbach, Germany," *The New York Times*, August 4, 2016, https://www.nytimes.com/2016/08/05/world/europe/germany-refugees-terrorism.html.

[115] Bridget Moreng, "ISIS' Virtual Puppeteers," *Foreign Affairs*, September 21, 2016.

[116] Amarnath Amarasingam, "An Interview with Rachid Kassim, Jihadist Orchestrating Attacks in France," *Jihadology*, November 18, 2016, https://jihadology.net/2016/11/18/guest-post-an-interview-with-rachid-kassim-jihadist-orchestrating-attacks-in-france/.

[117] Henry Samuel, "Man Held over Jihadist Murders of French Police Couple After 'DNA Found on Their Computer,'" *The Telegraph* (London), December 11, 2017, https://www.telegraph.co.uk/news/2017/12/11/france/.

Live, saying: "I don't know yet what I'm going to do with him." Abdalla had previously been arrested in 2013 for his involvement in a jihadist recruiting network.[118]

July 2016

- Kassim was in contact via Telegram with Adel Kermiche and Abdel Malik Nabil Petitjean, who slit the throat of an elderly priest during services at a church in St. Ètienne-du-Rouvray. Authorities believe Kassim introduced the two operatives, who lived over 400 miles apart and first met in person shortly before the attack. Kassim took over Kermiche's Telegram account after he was killed by police, one indication of his importance to the attackers.[119]

September 2016

- Kassim was in contact with a 15-year-old French boy who planned to carry out a knife attack in Paris.[120]

October 2016

- Kassim was in contact with an 18-year-old who was arrested in Clichy-la-Garenne (Hauts-de-Seine) for plotting an attack.[121]

- Kassim was in contact via Telegram with a young couple in Noisy-le-Sec who were planning an attack. Authorities arrested them after determining that their attack was imminent.[122]

In addition to his role in these various plots, Kassim succeeded in bringing disparate individuals together to form cells (as he seemingly did for the attackers in the aforementioned St. Ètienne-du-Rouvray church attack). In September 2016, French authorities arrested a group of female terrorists who tried but failed to set off a car bomb near Paris's Notre Dame Cathedral. One of them stabbed an officer outside the Boussy-Saint-Antoine rail station as authorities made the arrest.[123] Before the attempted attack, none of the women had had any type of relationship with one another. Instead, they were brought together solely by Kassim.[124]

In connecting the women, Kassim merged two different lines of terrorist effort in two different parts of France based on one operative's reluctance to carry out a suicide operation. Sarah Hervouët, a 23-year-old convert to Islam who was planning an attack in the southeastern French commune of Cogolin, had been communicating with Kassim over Telegram. Acting on Kassim's orders, Hervouët drafted her will, wrote farewell letters to relatives, and made a video proclaiming her

---

[118] Angelique Chrisafis, "French Police Chief and Partner Killed in Stabbing Claimed by ISIS," *The Guardian* (London), June 14, 2016, https://www.theguardian.com/world/2016/jun/13/french-policeman-stabbed-death-paris.
[119] Moreng, "ISIS' Virtual Puppeteers."
[120] "French Police Arrest Teenager Over 'IS Terror Plot,'" *BBC*, September 14, 2016, https://www.bbc.com/news/world-europe-37364222.
[121] "Menace terroriste: le jeune homme arrêté à Clichy a été mis en examen et écroué," *Le Parisien* (France), October 4, 2016, http://www.leparisien.fr/faits-divers/terrorisme-un-homme-soupconne-de-vouloir-commettre-une-attaque-mis-en-examen-et-ecroue-04-10-2016-6175613.php.
[122] Romina McGuinness, "French Terror: Man and Pregnant Girlfriend Arrested in France Over Terror Attack Plot," *Express* (U.K.), October 17, 2016, https://www.express.co.uk/news/world/722150/FRENCH-TERROR-Man-pregnant-girlfriend-arrested-ISIS-plots-France.
[123] Conor Gaffey, "Notre Dame Gas Plot: Three Women With Suspected ISIS Links Under Investigation," *Newsweek*, September 13, 2016, https://www.newsweek.com/notre-dame-gas-plot-three-women-isis-links-investigation-497760.
[124] Moreng, "ISIS' Virtual Puppeteers."

allegiance to Daesh. But she lost her appetite for this "suicide-by-police" attack. So Kassim connected her with two other women preparing to carry out an attack in Paris instead.[125] Though the women failed to carry out the dramatic attack that Kassim hoped for, the Notre Dame case demonstrates the speed, agility, and adaptability of the virtual plotter model.

Bahrun Naim. One of Daesh's top Indonesian militants, Bahrun Naim, was also one of the its most prolific Southeast Asian virtual plotters. He ran a blog and frequently posted on a Telegram channel titled "Explosive and Electrochemistry Division," which provided advice on a litany of topics of interest to militants, including bombmaking and money laundering.[126] Naim even released a 47-page manual titled *Nuclear for Dummy* [sic], which included a tutorial on how to build an unconventional, or "dirty," bomb.[127] Prior to his death in June 2018, Naim was involved in numerous plots across Southeast Asia, including the following:

- **August 2015**: Naim provided funding to three militants who planned to bomb a Buddhist temple, a church, and police stations in Solo, Indonesia on August 17. The militants were arrested prior to carrying out the attack. They appear to have chosen August 17 because it is Indonesia's Independence Day.

- **December 2015**: Naim provided funding and direction to Arif Hidayatullah, an Indonesian militant who wanted to carry out an attack around the New Year. He reportedly sought to attack Jewish and Shia targets, as well as prominent political leaders.[128] Authorities discovered bomb-making materials when they arrested Hidayatullah.[129]

- **January 2016**: Indonesian authorities believe Naim was the mastermind behind an attack in Jakarta that killed four civilians. The attack, which struck the city's downtown area, employed bombs and guns.[130]

- **June 2016**: Naim was in contact with four Indonesian men who were convicted of planning to bomb a Buddhist temple in Solo, Indonesia. Naim reportedly provided them with funding. By the time of their arrest, they had already built the bomb that they intended to use in their attack.[131]

- **July 2016**: Naim reportedly instructed Indonesian militant Nur Rohman to conduct a suicide bombing on the Surakarta City Police headquarters. Rohman died in the attack, but only managed to wound one police officer in the process.[132]

---

[125] Soren Seelow, "Sarah Hervouet, 23, Would-Be Martyr [French]," *Le Monde*, October 11, 2016.
[126] Naim's blog was titled "Bahrun Naim: Analis, Strategi dan Kontra Intelijen," which translates to *Bahrun Naim: Analysis, Strategy and Counter Intelligence.*
[127] See discussion in Tom Allard & Agustinus Beo Da Costa, "Indonesian Militants Planned 'Dirty Bomb' Attack," *Jakarta Globe* (Indonesia), August 25, 2017.
[128] Rohan Gunaratna, "Life and Death of Bahrun Naim: SE Asia's Most Wanted Terrorist," *Benar News* (Indonesia), October 3, 2018, https://www.benarnews.org/english/commentaries/asia-pacific-threat-update/bahrun-death-10032018124337.html.
[129] Francis Chan & Wahyudi Soeriaatmadja, "ISIS Funded Attack in Jakarta," *The Straits Times* (Singapore), March 5, 2016.
[130] "4 Indonesians Jailed over IS-Linked Terror Plot," *Channel News Asia* (Singapore), June 15, 2016.
[131] Ibid.
[132] Muh Taufiqurrohman, "From Radical to Terrorist: The Man Behind Five Terror Plots in Indonesia," *TODAY Online* (Singapore), December 15, 2016.

- **August 2016**: Indonesian police disrupted a cell in Batam coordinating with Naim to launch a rocket attack on Marina Bay. Authorities said members of the Batam cell "had been measuring elevation points and the distance from the hill to their target in Singapore."[133] Naim reportedly planned to deploy technicians afterward to make explosives and prepare for the attack.

- **December 2016**: Naim provided funding and tactical instruction to four Indonesian militants who were planning to conduct a bombing at the Merdeka Palace, a presidential palace in Jakarta. The bomber was supposed to have been the only woman in the cell, Dian Novi Yulia.[134]

- **October 2017**: A five-person Indonesian cell calling itself "Young Farmer" sought to build and detonate a chemical bomb at the presidential palace and a police command post in Jakarta. The bomb was constructed in accordance the instructions on Naim's blog. It is unclear if Naim had direct contact with this cell.[135]

Daesh's successful implementation of the virtual plotter model ultimately allowed the group to seize strategic ownership over what would previously have been considered disparate "lone wolf" attacks. By creating a bridge between potential militants and the organization, virtual plotters empower lone actors to advance Daesh's objectives at little expense to the organization. Each attack showcases Daesh's global reach. In this way, virtual plotters help to maximize the psychological and reputational effects of violence committed in Daesh's name.[136]

Competition

It is difficult to pinpoint the precise beginning of the *competition* phase. Social media companies faced pressure to remove Daesh content from their platforms shortly after the group emerged as a global phenomenon, but the companies' early efforts were often lackluster. Daesh began to face significant resistance on popular social media platforms around mid-2015.

Early on, Facebook, Twitter, and other social media sites struggled to contend with the sheer amount of content requiring removal. This prompted them to pursue technological approaches to removing pro-Daesh content from their platforms. These companies gravitated toward employing artificial intelligence to proactively identify proscribed content.[137] This change reduced reliance on

---

[133] Wahyudi Soeriaatmadja, "Suspected Batam Launch Site of Foiled Rocket Attack was 18km away from Marina Bay," *The Straits Times* (Singapore), September 27, 2016, https://www.straitstimes.com/asia/se-asia/suspected-launch-site-of-foiled-rocket-attack-was-18km-away-from-marina-bay.

[134] Ray Jordan, "These are the Faces of Two Terrorist Suspects Who Brought Bomb to 'Bride' Dian," *Detikcom* (Indonesia), December 12, 2016.

[135] "Densus Hold Reenactment of 'Young Farmer' Terrorism Case," *Damailah Indonesiaku* (Indonesia), October 26, 2017.

[136] Though the number of virtually plotted attacks appears to have dwindled recently, Daesh may at some point reinvigorate its virtual plotting apparatus. Alternatively, another militant group that employs terrorism may adopt or seek to improve the virtual plotter model.

[137] Julia Carrie Wong, "Twitter Announces Global Change to Algorithm in Effort to Tackle Harassment," *The Guardian* (London), May 15, 2018, https://www.theguardian.com/technology/2018/may/15/twitter-ranking-algorithm-change-trolling-harassment-abuse; see also Twitter's "Twitter Rules Enforcement" (n.d.),

users or employees to manually report content, and vastly increased the speed with which content could be removed.

In this way, social media companies' capability to execute takedowns of pro-Daesh material—and ultimately, of material supporting a variety of other violent and non-violent extremist groups—have dramatically improved. So too has the willingness of these companies, some of which once espoused absolutist positions about allowing all voices onto their platforms,[138] to use these capabilities in a variety of contexts. Twitter suspended over 1.2 million accounts for "terrorist content" between August 2015 and December 2017; Facebook removed 14.3 million "pieces of content related to [Daesh], al-Qaeda, and their affiliates" in the first three quarters of 2018; and YouTube removed over 60,000 videos for violating its "policies against violent extremism" from September-December 2018.[139] Such removals and suspensions have had a tangible impact on Daesh's reach. As J.M. Berger and Heather Perez showed in a 2016 study, Twitter's suspensions proved detrimental to both the number of followers and amount of content associated with Daesh accounts. Even when accounts returned under a similar name, they struggled to gain the same amount of followers that they enjoyed prior to their suspension.[140]

Even less mainstream platforms that often present themselves as free-speech purists have succumbed to pressure to combat terrorists' use of their services. Telegram announced a new privacy policy in August 2018 that would, for the first time, allow it to provide user information to authorities. Per Telegram CEO Pavel Durov, the policy change "is another measure we've taken to discourage terrorists from abusing our platform."[141]

For now, counter-Daesh measures have significantly disrupted the group's exploitation of social media. But the future of the competition phase depends in large part on developments that will both be technological in nature and also related to the broader environment of online communications. Will Daesh continue to be denied access to major social-media platforms that could again allow it to reach truly massive audiences? Will a platform with expressly libertarian principles that will not remove terrorist content—something akin to the controversial site Gab—gain enough popularity that Daesh is able to rehash its Twitter salad days? Or will Daesh find another way to game the social-media companies' community standards and push its message out—perhaps through pro-

---

https://transparency.twitter.com/en/twitter-rules-enforcement.html, which provides detailed statistics related to account suspensions in six-month increments.

[138] One particularly galling example is the Twitter executive who said of Daesh in late 2014: "One man's terrorist is another man's freedom fighter." Jenna McLaughlin, "Twitter is not at War with ISIS. Here's Why," *Mother Jones*, November 18, 2014, https://www.motherjones.com/politics/2014/11/twitter-isis-war-ban-speech/. By the time the executive's words were printed, Daesh had already 1) beheaded multiple people in videos that were distributed via a variety of media, including Twitter, 2) launched a literal campaign of genocide against the Yazidi religious minority, and 3) publicly boasted that they were holding women as sex slaves.

[139] See Twitter Public Policy, "Expanding and Building #TwitterTransparency," April 5, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/twitter-transparency-report-12.html; Monika Bickert, "Hard Questions: What Are We Doing to Stay Ahead of Terrorists?," Facebook, November 8, 2018, https://newsroom.fb.com/news/2018/11/staying-ahead-of-terrorists/; YouTube, "YouTube Community Guidelines Enforcement," (n.d.), https://transparencyreport.google.com/youtube-policy/featured-policies/violent-extremism?policy_removals=period:Y2018Q4&lu=policy_removals.

[140] J.M. Berger and Heather Perez, *The Islamic State's Diminishing Returns on Twitter: How Suspensions Are Limiting the Social Networks of English-Speaking ISIS Supporters* (Washington, DC: George Washington University, 2016).

[141] Christopher Miller, "Telegram CEO Defends New Privacy Policy, Says Data is Still Safe," *Radio Free Europe/Radio Liberty*, August 28, 2018, https://www.rferl.org/a/telegram-ceo-defends-new-privacy-policy-says-user-data-still-safe/29458179.html.

Daesh individuals masquerading as neutral third parties who stop just short of warranting a suspension by major platforms? Or will a combination of national-level regulations and improvements in artificial intelligence mean that Daesh's message never again reaches the heights that it once knew?

These questions illustrate why we do not know the outcome of the competition phase following VNSAs achieving the breakthrough phase on the adoption curve: The uncertainties of the technological environment mean there are more questions than answers.

VNSAs' Adoption of Drones

The allure of unmanned systems (UMS), and specifically unmanned aerial systems (UAS), for VNSAs dates back over 25 years. The reason for this allure is straightforward, as the technology offered an opportunity for groups to develop a weapon that would be effective in a dimension of warfare that had previously been beyond reach to them: the air. The introduction, proliferation, and decrease in price of commercially-available unmanned systems has represented a boon for VNSAs, which have increasingly employed this technology for diverse ends.

In his 2016 report *Remotely Piloted Innovation*, Don Rassler developed a typology of how VNSAs have employed UAS. His typology is broadly applicable to all UMS, and it is instructive in explaining how VNSAs have used these systems previously, as well as how they may adapt and innovate in the future. The five categories of use in his typology are: surveillance, strategic communications, smuggling, disruption, and weaponization.[142] As of the writing of this report, few, if any, individual VNSAs have effectively employed UMS in all five ways.

The availability of increasingly advanced UAS at declining practices appears most significant to VNSAs' decision to seek out and employ such technology. But there are also several other relevant factors, including the environment a group operates in, its technical aptitude, its ideology, its organizational structure, and the resources and physical sanctuary the group enjoys. For example, part of the reason Daesh was so effective in developing and deploying its UAS program was the terrain in Syria and Iraq. Deserts and urban environments lend themselves to the use of UAS for intelligence, surveillance, and reconnaissance (ISR) in a way that, for example, heavily forested areas do not.

As we discuss subsequently, even groups that had significant resources in the 1990s and early 2000s were, in the absence of assistance from a state actor, unable to effectively use UMS, either for ISR or as a weapon. But the more recent rapid improvement in commercially-available UAS technology over the past eight to ten years has allowed VNSAs to traverse the adoption curve. While the most prolific contemporary user of weaponized UAS, Daesh, has lost its physical territory—and with it, at least some of its ability to refine its UAS program—there is no reason to believe that drones will cease to play a role in the group's strategic thinking and planning. In the following sections, we detail various VNSAs' efforts to develop UMS programs, focusing on how commercially-available technology aided or inhibited these efforts.

Early Adoption: 1994 to 2005

The early adoption stage in VNSAs' use of UMS is characterized by larger, more well-resourced VNSAs' first forays into the use of unmanned systems. Commercial options at the time provided them with little more than expensive and ineffective distractions.

One of the earliest attempts to weaponize UAS was by the Japanese cult Aum Shinrikyo in 1994. The cult was led by Shoko Asahara, who preached a millenarian hybrid of Buddhism and Christianity focused on a coming apocalypse. When Aum emerged in Japan, it was one of many new and cult-like religious movements active in the country, with the rise in these movements driven by a

[142] Don Rassler, *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology* (West Point, NY: Combatting Terrorism Center, 2016), https://ctc.usma.edu/remotely-piloted-innovation-terrorism-drones-and-supportive-technology/.

growing sense of isolation and alienation amidst a period of significant technological, economic and social change.[143] Anchored in a belief in Asahara's enlightenment and prophetic ability, some of the more outlandish practices described by former cult members included paying "handsomely for rituals involving Asahara's hair and bathwater," with one former member explaining that he paid "more than £6,115 ($8,100) in 1988 for a 'blood initiation' where he drank what was said to be the leader's blood."[144]

Aum developed a chemical and biological weapons program, as well as several methods to disperse the weapons. The cult sought out a remote dispersal mechanism due to the volatile nature of the rudimentary weapons that it built, and experimented with a remote-controlled helicopter retrofitted to spray sarin gas in a targeted assassination. All the experiments were unsuccessful, with the helicopter crashing on their second attempt.[145]

The group's inability to weaponize a remote-controlled helicopter is significant, and indicative of the crude state of UMS/UAS technology at the time, as Aum had copious resources available and its members had an extremely high level of technical aptitude. Aum's financial resources were estimated to be upwards of $1.5 billion at their peak—and the group enjoyed a stable base of operations in Japan, where the cult owned property in several cities, and operated a number of businesses, including a computer manufacturing company.[146] Aum members included physicists, chemists and doctors educated at Japan's top universities, and the group even operated its own hospital in Tokyo. Many skilled members were drawn into a designated "Science and Technology Agency" responsible for Aum's chemical weapons program.[147]

In March 1995, Aum carried out a major attack on the Tokyo subway system using sarin gas. It followed an earlier sarin attack in 1994 in another Japanese city, in which Aum targeted judges presiding over a real estate dispute involving the group.[148] In the 1995 Tokyo attack, the Aum operatives placed five packages containing sarin on subway trains, then punctured them to release the sarin as the trains converged on stations near the Japanese parliament. Nearly 3,800 civilians were exposed to the sarin, around a thousand required hospitalization, but fortunately only 12 people were killed.[149] When Japanese authorities raided Aum's properties, they found a lab capable of producing chemical weapons at an industrial scale, suggesting the group's potential to orchestrate further attacks.[150]

Following Aum's attempt to use a UAS, there was little confirmed VNSA use of UAS until the early 2000s. During this period, at least three VNSAs showed clear interest in UAS programs:

---

[143] Mark Bowden and Loretta Tofani, "The Cult of Doom's Strange Rise," *The Philadelphia Inquirer*, April 16, 1995.
[144] "Aum Shinrikyo: The Japanese Cult Behind the Tokyo Sarin Attack," BBC, July 6, 2018, https://www.bbc.com/news/world-asia-35975069.
[145] Tim Ballard et al., *Chronology of Aum Shinrikyo's CBW Activities* (Monterey, CA: James Martin Center for Nonproliferation Studies at Middlebury Institute for International Studies, 2001), http://www.nonproliferation.org/wp-content/uploads/2016/06/aum_chrn.pdf.
[146] Kyle Olson, "Aum Shinrikyo: Once and Future Threat?," *Emerging Infectious Diseases* 5:4 (August 1999), https://wwwnc.cdc.gov/eid/article/5/4/99-0409_article.
[147] Kwan Weng Kin, "Scientists, Doctors Among Japanese Sect's Science Team," *The Straits Times*, April 5, 1995.
[148] Olson, "Aum Shinrikyo."
[149] Ibid.
[150] Ibid.

Lashkar-e-Taiba (LeT), the Revolutionary Armed Forces of Colombia (FARC), and Hizballah.[151] With the exception of Hizballah's efforts, much of the reporting on these early programs is murky, and details are hard to verify.

The first North America-based activity involving VNSAs and UAS occurred in early 2002, when members of what later came to be called the "Virginia Jihad Network" tried to procure components for a UAS program that LeT was in the early stages of developing. Eleven members of the network were arrested in 2003, with charges brought against them including provision of material support to LeT and attending training camps in Pakistan. At least one member of the group traveled from Virginia to Colorado to obtain what emails exchanged within the group described as "long range remote controls and any other vidioe [sic] systems."[152] Cell members also successfully purchased a system designed to allow a UAS operator to input GPS coordinates and have the system navigate to those coordinates autonomously.[153] Despite the promise of this seemingly advanced system, none of the technology worked as intended, as evidenced by anguished emails that cell members sent to the vendors from whom they had purchased relevant technologies.[154]

In late 2002, Colombian troops raided two FARC camps and found nine model aircraft, which the Colombian government alleged were to be filled with explosives and flown into a nearby oilfield. There was little subsequent media coverage of this incident, but the basic idea of the plot—explosives in a model airplane targeting poorly protected infrastructure—foreshadows the designs used in a number of plots in the subsequent *iteration* phase of the VNSA adoption curve for UAS technology.

As to Hizballah, the group's early success with UAS is attributable in large part to Iranian patronage and technology transfer. During this period, Hizballah's use was restricted to ISR missions, as opposed to utilizing drones to carry out attacks. The first publicized instance of Hizballah deploying a drone occurred in late 2004, when a Hizballah drone flew over Israeli towns in the western Galilee.[155] A few months later, another Hizballah UAS penetrated roughly 18 miles into Israeli airspace, then safely returned to Lebanon before it could be intercepted. Both UAS used in these incidents were identified as Iranian, and open-source reporting indicates that the country's Islamic Revolutionary Guard Corps had not only provided the drones to Hizballah, but also facilitated training on the systems for Hizballah operatives.[156] Despite Hizballah's leader Hassan Nasrallah claiming at the time that the group had drones capable of carrying a "40 to 50 kilogram" payload, weaponization had not yet occurred.[157]

---

[151] Several other alleged plots or programs are mentioned in other reports, but the sourcing is suspect. Don Rassler reaches a similar conclusion to ours in his 2016 report. See Rassler, *Remotely Piloted Innovation*, p. 5.

[152] Indictment, *United States v. Chandia*, 1:05-CR-401 (E.D. Va., September 14, 2005), https://www.investigativeproject.org/documents/case_docs/1087.pdf.

[153] Ibid.

[154] For example, an email sent on May 4, 2002, read: "I JUST TRIED THE EQUIPMENT AND THE SYSTEM IS NOT WORKING AS IT WAS SAID, THE GIVEN RANGE IS NOT BEING SATISFIED, IT WAS SAID TO BE ADEQUATE FOR 5 [MILES] RANGE BUT AFTER 200 METERS IT [LOSES] RECEPTION AND WITHIN 200 METERS INTERFERENCE WAS ALSO THERE. CAN U ADVICE REGARDING THESE ISSUES OR CAN U EXPLAIN THE PROCESS OF RETURNING THE GOODS." Ibid, p. 16.

[155] "Hezbollah Drone Flies Over Israel," BBC, November 7, 2004, http://news.bbc.co.uk/2/hi/3990773.stm.

[156] Yoav Stern & Ze'ev Schiff, "Report: Iran Admits to Supplying Hezbollah with Drones," *Haaretz* (Israel), November 10, 2004.

[157] "Hezbollah Says It Has Capability to Bomb Israel From the Air," *Haaretz* (Israel), November 12, 2004, https://www.haaretz.com/1.4754267.

Thus, unlike the other VNSA early adopters of drones, Hizballah benefited from the direct transfer of technology and training from a state actor. But one indication of the relatively crude state of the technology at the time is the fact that even with state support, Hizballah's use of UAS can still only be considered a partial success during this period. While it was able to fly drones over Israeli territory without the Israelis shooting them down, it did not obtain any discernible strategic or tactical advantage from its possession of UAS at this time, other than perhaps the psychological edge that comes from these drone flights.

Iteration: 2005 to 2014

During the iteration phase, VNSAs began to incrementally improve on their initial designs, and the probability of successful weaponization grew as commercially available technology improved. By the end of this period, more advanced VNSAs established substantial ISR capabilities, VNSAs that enjoyed state support had successfully weaponized UASs, and criminal networks around the world had begun to see the utility of UMS.

Four UMS-related terrorist plots of varying levels of sophistication were disrupted in Western countries during this period: a 2006 plot in Ohio that did not move beyond the exploratory phase; another in 2011 in Massachusetts; and two in Germany in 2013. There were also two recorded instances of al-Qaeda or affiliated groups outside the West making use of UAS during this period. Each of these uses foreshadowed future developments in VNSA use of UMS, while also underscoring the capabilities gap that continued to persist through most of the iteration period.

The first Western plot was disrupted in 2006 in Columbus, Ohio. Christopher Paul was a convert to Islam with associate degrees in computer electronics and electrical engineering. Paul spent much of the 1990s traveling between Ohio and conflict zones in Central Asia and the Balkans.[158] During his travels, Paul trained and fought in both Afghanistan and Bosnia, and managed to develop strong connections to significant jihadist figures.[159] At the time of his arrest, Paul was in possession of, among other things, explosives manuals and a modified remote-control boat, and he had conducted research on remote-controlled boats and helicopters.[160] Paul does not appear to have moved beyond the exploratory stage with these devices, and weaponizing a UMS was only one of several possible avenues for attack that he had been researching. Nonetheless, Paul's idea of avoiding a singular focus on aircraft and exploring the possible use of remote-controlled boats is consonant with future VNSA efforts.

The most significant plot against a Western target involving a drone occurred in 2011, when Rezwan Ferdaus, who had graduated from Northeastern University with a degree in physics, was arrested for a plot to target the Pentagon and U.S. Capitol building using remote-controlled model aircraft packed with explosives. Unlike Christopher Paul, Ferdaus moved beyond the ideational stage, and had obtained a model aircraft that he planned to retrofit to carry explosives. The plot involved launching several of these UASs, where they were intended to detonate when they hit their targets.

---

[158] Kirk Richards & Charlie Boss, "Terrorism Suspect Was Once 'Super Nice Kid,'" *Columbus Dispatch*, April 14, 2007, https://www.dispatch.com/content/stories/local/2007/04/14/PAUL14.ART_ART_04-14-07_A1_N46CM82.html.

[159] Department of Justice, press release, "Ohio Man Pleaded Guilty to Conspiracy to Bomb Targets in Europe and the United States," June 3, 2008, https://www.justice.gov/archive/opa/pr/2008/June/08-nsd-492.html.

[160] Indictment, *United States v. Paul*, 2:07-CR-00087 (S.D. Ohio, April 7, 2007), https://www.investigativeproject.org/documents/case_docs/585.pdf.

Ferdaus described his plot in megalomaniacal terms, saying that it would "severely disrupt ... the head and heart of the snake," a reference to the U.S. government.[161] To establish his credibility with undercover agents posing as members of al-Qaeda, Ferdaus manufactured a number of remote detonators that he believed insurgents in Iraq would use in improvised explosive devices (IEDs).[162]

Ferdaus believed he could acquire remote-controlled planes capable of carrying a payload of up to 20 kilograms.[163] In reality, the models he ended up obtaining were significantly less appropriate for the plot. They only had an estimated 2.5-kilogram payload.[164] And even if his planes had been able to handle the payload, the heavier takeoff weight would have required a large open area for takeoff, and would have made maneuvering the aircraft much harder.

Ferdaus's key innovation was his desire to use a commercially-available GPS autopilot system and Google Earth to navigate the aircraft toward their targets. This stood in contrast to line-of-sight navigation, which had plagued previous VNSA attempts to weaponize remote-controlled aircraft. Ferdaus described the logistics of his plot as follows: "My plan is to have a fast model airplane with a GPS system stuffed with handhelds and it's on a timer and it ... has the coordinates of the targets.... All it has to do crash into the target."[165] While the plot's ultimate likelihood of success was questionable even if Ferdaus had not been caught by authorities, it is clear that many aspects of his plot foreshadowed future threats.

One of the German plots involved a group of students who were originally from Tunisia, some of whom were studying aerospace engineering together. They were seemingly working on a GPS system that could remotely guide UASs to a target.[166] The second plot disrupted by German police involved a cell of right-wing extremists who were plotting to use a UAS to attack a summer camp.[167] There is extremely limited publicly-available information about both cases. However, the details of the plot involving students show that remote navigation remained an important concept for individuals interested in employing UAS for terrorist attacks.

Shortly after these two plots were disrupted, a member of the German Pirate Party flew a drone within a few meters of German Chancellor Angela Merkel at a campaign rally, in what he described as a protest against government surveillance.[168] But the protest also demonstrated how vulnerable individuals—even high-profile politicians with security details—were to UAS attacks.

---

[161] Affidavit of Special Agent Gary S. Cacace, *United States v. Ferdaus,* 1:11-CR-10331 (D. Mass., September 29, 2011), https://www.investigativeproject.org/documents/case_docs/1690.pdf.

[162] Ibid.

[163] Ibid.

[164] "Could Model Airplanes Become a Terrorist Weapon?," Associated Press, September 29, 2011.

[165] Affidavit of Special Agent Cacace, *United States v. Ferdaus*. Cacace's affidavit explains that Ferdaus would sometimes refer to grenades as "handhelds."

[166] "German Police Shoot Down Model Plane Terror Plot," *Der Speigel* (Germany), June 25, 2013, https://www.spiegel.de/international/germany/german-police-suspect-remote-controlled-airplane-terror-plot-a-907756.html.

[167] Jack Nicas, "Criminals, Terrorists Find Uses for Drones, Raising Concerns," *Wall Street Journal*, January 29, 2015, https://search.proquest.com/globalnews/docview/1648740492/CA1746F898CB472CPQ/1?accountid=14771. "Police recovered bomb-making materials and a drone from the right-wing extremists, who were allegedly planning to use the device to bomb a German summer camp, according to the presentation"

[168] Sean Gallagher, "German Chancellor's Drone 'Attack' Shows the Threat of Weaponized UAVs," *ArsTechnica*, September 18, 2013, https://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/.

The final plot from this period was an alleged chemical weapon plot involving members of Daesh who were arrested in Iraq in June 2013. The Iraqi government alleged that the plotters intended to disperse sarin and mustard gas from remote-controlled helicopters.[169] According to Iraqi officials, the cell intended to carry out attacks in Iraq, and also smuggle the technology and weapons to plotters in North America and Europe.[170] The plot is significant for two reasons. First, it shows that even prior to declaring its caliphate in mid-2014, Daesh was actively considering the role UAS could play in its operations. Second, at least in the MENA region, the technology was still not as effective and affordable as the plotters would prefer. The remote-controlled helicopters displayed by the Iraqi government at a press conference detailing the arrests were small, and most likely lacked the capacity to carry a chemical weapon dispersal device up to a mile away. As was the case with Aum Shinrikyo almost 20 years earlier, it was still easier for VNSAs to manufacture rudimentary chemical weapons than to effectively use available UMS technology.

During this period of iteration, other VNSAs began to take an interest in using UMS, including criminal organizations and cartels who sought to incorporate drones into their smuggling operations. Such organizations experimented with commercially available systems, and also undertook early experiments in developing their own platforms.[171] The first use of UMS in smuggling was detected 2011, and between 2012 and mid-2014, the U.S. Drug Enforcement Agency detected an average of 150 drone flights a year that were used to transport cocaine and other drugs across the border from Mexico into the United States.[172]

Key Takeaways from the Iteration Period. During this period, less sophisticated VNSAs faced four key barriers to successful development and use of UAS: UAS had a limited range, they were hard to control, the payload of fixed-wing remote-control planes was limited, and advanced models were expensive. Subsequent movement along the adoption curve would necessitate a change in at least one of these domains.

Breakthrough: 2014 to 2018

Several factors contributed to the breakthrough in VNSA use of UAS that began around 2014. Critical on the technological side was the introduction and exponential growth of affordable, easy-to-operate quadcopter drones like those produced by Chinese manufacturer SZ DJI Technology.[173] The first version of DJI's most popular model, the Phantom, was introduced in January 2013. The press release that accompanied its launch stated: "Flight parameters and functions have been [set up] and tuned by DJI engineers, so you can fly your Phantom the moment you receive it. It is so easy to operate and stable."[174] Just as it is clear why this was good news for hobbyists, so too should its utility for VNSAs be apparent. In a short period, the technological barriers that had stymied VNSA adoption

---

169 Rami Ruhayem, "Iraq Uncovers al-Qaeda 'Chemical Weapons Plot'," BBC, June 1, 2013, https://www.bbc.com/news/world-middle-east-22742201.

170 Ibid.

171 "Carteles Hacen Drones para Trasiego Hacia EU," *El Universal* (Mexico), July 10, 2014.

172 Ibid.

173 Quadcopter drones are a four-rotor unmanned system, where the rotors are arranged around the body of the aircraft. The number of rotors on a drone tends to correlate with overall power and payload capacity. Multi-rotor systems are also more stable *vis-à-vis* a single rotor.

174 DJI Technology, press release, "DJI Releases All-in-One Solution, Read-to-Fly 'Phantom' Quadcopter," January 7, 2013, https://www.dji.com/ca/newsroom/news/dji-releases-all-in-one-solution-read-to-fly-phantom-quadcopter.

of UMS technology fell. The generation of drones released beginning in 2013 represented a product that was of immediate use to VNSAs.

This generation of UASs found a broader customer base than previous generations of more niche remote-controlled aircraft, which were the domain of a small community of hobbyists. The Consumer Technology Association estimated that global commercial drone sales rose from 128,000 units in 2013 to 1.14 million units only two years later, in 2015.[175] The growing popularity of drones has continued to the present, with the U.S. Federal Aviation Administration estimating the compound annual growth rate in the United States to be roughly 40%.[176] At the same time, a number of highly capable VNSAs managed to build structures conducive to adapting this consumer technology.

The Strengths of VNSA Bureaucracy in Repurposing Drones to the Groups' Purposes. As discussed in this report's preceding section on virtual plotters, Daesh's organizational structure rendered it well-suited for repurposing consumer technologies to advance its objectives.[177] Similar to the bureaucratization of the Amniyat al-Kharji, Daesh's UAS program was housed under its Committee of Military Manufacturing and Development (CMMD) and assigned to the Al-Bara' bin Malik Brigade. This Brigade was initially formed to focus on suicide operations, with its roots stretching back to 2005.[178] The CMMD was responsible for standardizing much of Daesh's military manufacturing. A 2016 report by Conflict Armament Research found that Daesh had built an organization capable of standardizing munition production across its factories, thus ensuring interoperability. This required a high degree of bureaucratization and structure.[179]

Daesh's bureaucracy played an important role in guiding the group's acquisition of complete UAS systems and specialized components that it could incorporate into commercially-available or purpose-built platforms. Some of its foreign supporters played an integral role as well. One of the group's well-developed supply chains about which there is significant available open-source information involved British brothers Ataul Haque Sujan and Siful Sujan.[180] While Siful Sujan moved to Syria and became a high-ranking Daesh member, Ataul remained in Europe, and establshed contact with Daesh virtual plotter Junaid Hussain, who was discussed at length in the previous section of this report. The brothers used a series of legitimate businesses (iBacsTel and subsidiaries, which sold remote printers and point of sale systems) to procure UMS systems and components, and then ship

---

[175] Craig Issod, "Drone Sales Forecasts Released by CTA," *DroneFlyers*, July 17, 2016, https://www.droneflyers.com/drone-sales-forecasts-released-cta/.

[176] Federal Aviation Administration, *Unmanned Aircraft Systems* (2017), p. 40, https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/Unmanned_Aircraft_Systems.pdf.

[177] Other VNSAs active in Syria and Iraq have also made use of drones in offensive operations. See, for example, Peter Dockrill, "First-Ever Drone Swarm Attack Has Struck Russian Military Bases, Sources Claim," *Science Alert*, January 11, 2018, https://www.sciencealert.com/swarm-home-made-drones-strike-military-base-first-attack-kind-russia-uavs.

[178] See Don Rassler, Muhammed Al-'Ubaydi & Vera Mironova, *The Islamic State's Drone Documents: Management, Acquisitions, and DIY Tradecraft* (West Point, NY: Combating Terrorism Center, 2017), https://ctc.usma.edu/ctc-perspectives-the-islamic-states-drone-documents-management-acquisitions-and-diy-tradecraft/; Bill Roggio, "Al Baraa Ibn Malik Martyrdom Brigade Forms in Syria," *Long War Journal*, February 18, 2012, https://www.longwarjournal.org/archives/2012/02/al_baraa_ibn_malik_martyrdom_b.php (noting the Al-Bara' bin Malik Brigade's formation in Iraq in May 2005).

[179] Conflict Armament Research, *Standardisation and Quality Control in Islamic State's Military Production* (London, UK: Conflict Armament Research, December 2016), http://www.conflictarm.com/dispatches/standardisation-and-quality-control-in-islamic-states-military-production/.

[180] Jamie Merrill, "An FBI Probe, an IS Plot, and a Welsh Firm Caught in the Fallout," *Middle East Eye*, August 19, 2017, https://www.middleeasteye.net/news/revealed-fbi-probe-plot-and-welsh-firm-caught-fallout.

them to Syria.[181] Relevant to Daesh's movement along the adoption curve, the earliest purchases (2014) by the iBacsTel network primarily involved components needed to manufacture home-built systems, as opposed to commercial ones. The network later shifted its focus in 2015 to buying complete, commercially-available systems.[182] This sequencing underscores the continuing importance of advances in commercial platforms to VNSAs' use of the technology. It is worth carefully watching whether advances in other cutting-edge technologies, like 3D printing, will change this dynamic.

On the operational side, Daesh's bureaucratic structure included formalized tracking of each UAS mission, which required operators to record the type of mission and its location, and to complete a pre-flight checklist.[183] Gathering this data was important to allow the group to engage in organizational learning and improve its operations.

Daesh's Use of UAS. The earliest known uses of a UAS by Daesh after its rapid expansion in Syria and Iraq occurred in the spring and summer of 2014, when the group released propaganda videos featuring aerial shots of suicide vehicle-borne IEDs (VBIEDs) targeting the Syrian regime.[184] Aside from the propaganda value of these videos, this signaled that Daesh had obtained a capability—aerial surveillance—that had previously been the essentially exclusive domain of states. The group's increased awareness of the battlefield translated into an improved ability to scout targets, identify weaknesses, and improve the overall efficacy of Daesh's operations.

Over time, Daesh continued to refine its UAS capabilities, particularly as commercially-available UAS platforms, and the kind of surveillance they could undertake, continued to improve. Manufacturers of low-light/night vision cameras and forward-looking infrared cameras are now adapting their products for use on increasingly affordable commercial UAS platforms.[185] Daesh was able to gain its ISR capabilities for an exceptionally low price, compared to what other VNSAs paid for similar capabilities only a few years earlier. In 2011, during the height of Libya's rebellion against longstanding dictator Muammar Qaddafi, a Canadian drone manufacturer, Aeryon Labs of Waterloo, ON, provided at least two drones to the National Transitional Council (NTC) after Canada recognized the NTC as the legitimate government of Libya.[186] At the time, the drones were estimated to cost between $100,000 and $150,000 each, as compared to a DJI Phantom circa 2013, which could be had for less than $2,000.[187] The rapid decline in price, and increased quality of commercially available technology, broadened the number of VNSAs for whom the UAS was a useful and attainable technology.

---

[181] Don Rassler, *The Islamic State and Drones: Supply, Scale, and Future Threats* (West Point, NY: Combating Terrorism Center, 2018), p. 9, https://ctc.usma.edu/app/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf.
[182] Ibid., p. 13.
[183] Rassler, Al-'Ubaydi & Mironova, *The Islamic State's Drone Documents*.
[184] These videos have by now been removed from YouTube. For discussion of them, see Peter Bergen & Emily Schneider, "Now ISIS has Drones?," CNN, August 25, 2014, http://www.cnn.com/2014/08/24/opinion/bergen-schneider-drones-isis/index.html.
[185] See FLIR, press release, "FLIR and DJI Announce Strategic Collaboration to Enable Commercial Drones With Thermal Imaging Capability," December 10, 2015, http://investors.flir.com/news-releases/news-release-details/flir-and-dji-announce-strategic-collaboration-enable-commercial.
[186] Tu Thanh Ha, "How High-Tech Canadian Drones Gave Libyan Rebels a Boost," *The Globe and Mail*, August 23, 2011.
[187] Ibid.; cf. Sean Hollister, "DJI's Latest Phantom Drone Beams Aerial Footage to Your Phone," *The Verge*, October 31, 2013, https://www.theverge.com/2013/10/31/5053088/dji-phantom-2-vision-comes-with-camera-beams-to-smartphone (noting that a Phantom 2 Vision would cost $1,199).

The first known case of Daesh successfully weaponizing a UAS occurred in October 2016, when two Kurdish Peshmerga fighters died and two French soldiers were injured after a drone they shot down detonated.[188] An explosive inside the drone had been disguised as a battery.[189] This attack followed a series of attempts that used explosives attached to drones that were flown toward static positions, such as checkpoints. In these earlier attacks, either the drones did not detonate or else the detonation occurred long after the drone had been captured by coalition soldiers.

But shortly after Daesh's successful drone attack in October 2016, the group's weaponized drones rapidly proliferated. Fieldwork conducted by Conflict Armament Research in Ramadi suggested that the group's work on weaponization had been occurring for a significant period, with Daesh eventually reorienting its UAS program away from manufacturing entire drones toward re-purposing commercially-available technology.[190] The group settled on a more or less standardized approach to weaponization, which involved retrofitting commercially available drones. While Daesh experimented with fixed-wing versions, their most successful platforms appear to have been quadcopter drones with an underbody modification allowing them to carry grenades.[191] The grenades were primarily variants of a standard 40mm grenade, and were modified with custom-machined plastic fins to stabilize them in flight, a means the group adopted following experimentation with a number of possible variants.[192] The grenades were dropped from carriers under the drone operated by a small, inexpensive servo-motor.

Daesh's advanced ISR and weaponization was most apparent during the battle for Mosul in 2017, when its fighters used UAS to launch attacks and gain a dynamic picture of fighting in the city. Daesh used drones not only as a platform to conduct dozens of small-scale bombings each day, but also to guide mortar teams and direct suicide VBIEDS to their targets, providing them with directions in real-time through the city's narrow, winding streets.[193] In his later discussion of the liberation of Mosul, Gen. Raymond Thomas, the commander of the United States Special Operations Command (SOCOM) referred to Daesh's drones as the "most daunting" challenge for coalition forces. He explained the impact they had on coalition operations: "About five or six months ago, there was a day when the Iraqi effort nearly came to a screeching halt, where literally over 24 hours there were 70 drones in the air."[194]

Daesh's temporary control of airspace below a few thousand feet created significant hurdles for coalition forces, and rendered the coalition's more advanced aircraft ill-suited for the needs of ground forces. As one U.S. infantry officer who served in Mosul noted: "The jets and drones could

---

[188] Michael S. Schmidt & Eric Schmitt, "Pentagon Confronts a New Threat From ISIS: Exploding Drones," *The New York Times*, October 11, 2016, https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html.
[189] Charley Lanyon, "ISIS Uses Exploding Drones to Kill Kurdish Troops in First Successful Attack of Its Kind," *New York Magazine*, October 12, 2016, http://nymag.com/intelligencer/2016/10/isis-uses-exploding-drones-to-kill-kurdish-troops.html.
[190] Conflict Armament Research, *Frontline Perspective: Islamic State's Weaponised Drones* (London, UK: Conflict Armament Research, October 2016), www.conflictarm.com/download-file/?report_id=2416&file_id=2417.
[191] Nick Waters, "Death From Above: The Drone Bombs of the Caliphate," Bellingcat, February 10, 2017, https://www.bellingcat.com/news/mena/2017/02/10/death-drone-bombs-caliphate/.
[192] Ibid.
[193] Mike Giglio, "Inside the 'Mad Max-Style' Tactics ISIS Is Using in Its Last Stand in Iraq," *Buzzfeed*, March 9, 2017, https://www.buzzfeednews.com/article/mikegiglio/inside-the-mad-max-style-tactics-isis-is-using-in-its-last-s.
[194] David Larter, "SOCOM Commander: Armed ISIS Drones Were 2016's 'Most Daunting Problem,'" *DefenseNews*, May 16, 2017, https://www.defensenews.com/digital-show-dailies/sofic/2017/05/16/socom-commander-armed-isis-drones-were-2016s-most-daunting-problem/.

do [very little] about a DGI Phantom quad-copter, barely a cubic foot in volume, hovering over friendly forces and guiding the VBIED."[195] As VNSAs' access to, and skill in using, drones continues to improve, state actors are likely to face similar challenges.

Other VNSA Users. One of the more VNSA interesting uses of drones was a drone swarm launched against the Khmeimim airbase that Russian forces used in Syria on January 6, 2018. The swarm has not been conclusively attributed to a specific rebel group in open-source materials, though many observers suspect that it was launched by Hayat Tahrir al-Sham. Prior to the attack, a set of very similar drones were listed for sale in a Telegram channel used as an arms market by Syrian rebels.[196] This attack is differentiated by the use of a large number of homemade drones equipped with off-the-shelf GPS antennae that may have assisted the swarm in moving toward its target.[197] Nick Waters, a former British Army officer who monitors Syria for the open-source intelligence platform Bellingcat, wrote of the GPS in these drones: "The lack of cameras on the drones suggest that they are likely pre-loaded with a flight plan and then flown autonomously to their target."[198] Each drone had the capacity to drop up to ten bomblets. Though no Russian forces were killed in this attack—they were able to shoot the swarm out of the sky before—this attack represented a tactical evolution that will almost certainly be revisited in the future.

This period has also seen other VNSAs make use of drones, in particular the Houthis in Yemen's civil war. The Houthis have launched a series of successful attacks—including swarms in 2018 and 2019 against targets in Yemen and Saudi Arabia, and international tanker traffic in the Persian Gulf.[199] The frequency and success of these drone attacks is striking. For example, in a little less than a month, Abha Airport in Saudi Arabia's Asir Province was hit by Houthi drones at least three times. Early in the morning on June 14, the Houthis said they had launched drones against the airport, though no casualties were reported. On June 23, a Houthi drone killed one person and injured 21, in the airport. And on July 1, a Houthi drone injured nine people.[200] Over the same time period, at least 11 Houthi drones were intercepted by the Saudi military as they made their way across the country's border with Yemen.[201] Although the Saudis boast both the third largest military budget in

---

[195] Pablo Chovil, "Air Superiority Under 2000 Feet: Lessons from Waging Drone Warfare Against ISIL," *War on the Rocks*, May 11, 2018, https://warontherocks.com/2018/05/air-superiority-under-2000-feet-lessons-from-waging-drone-warfare-against-isil/.

[196] Adam Rawnsley & Christiaan Triebert, "Black Market Sold Drones Used in Russian Base Attack," *Daily Beast*, January 10, 2018, https://www.thedailybeast.com/black-market-sold-drones-used-in-russian-base-attack.

[197] Nick Waters, "The Poor Man's Air Force? Rebel Drones Attack Russia's Airbase in Syria," *Bellingcat*, January 12, 2018, https://www.bellingcat.com/news/mena/2018/01/12/the_poor_mans_airforce/.

[198] Ibid.

[199] Alessandro Arduino, "Houthi Attacks Signal New Chapter in Drone Warfare," *Arab Weekly*, May 26, 2019, https://thearabweekly.com/houthi-attacks-signal-new-chapter-drone-warfare.

[200] For reports on the three attacks, see "Yemen's Houthis Attack Saudi Abha Airport with Drones: Al Masirah TV," Reuters, June 13, 2019, https://www.reuters.com/article/us-yemen-security-saudi-attacks/yemens-houthis-attack-saudi-abha-airport-with-drones-al-masirah-tv-idUSKCN1TF01D; Jared Malsin, "Iran-Allied Houthis Expose Holes in Saudi Arabia's Missile Defense," *The Wall Street Journal*, June 25, 2019, https://www.wsj.com/articles/iran-allied-houthis-expose-holes-in-saudi-arabias-missile-defense-11561455002; Edward Yeranian, "Nine Civilians Wounded in Overnight Houthi Drone Attack on Saudi Arabia's Abha Airport," *Voice of America*, July 2, 2019, https://www.voanews.com/middle-east/nine-civilians-wounded-overnight-houthi-drone-attack-saudi-arabias-abha-airport.

[201] See "Saudi Forces Intercept Two More Houthi Drones," *Saudi Gazette*, June 18, 2019, http://saudigazette.com.sa/article/569190/SAUDI-ARABIA/Saudi-forces-intercept-two-more-Houthi-drones; "Saudi Arabia's Air Defense Forces Shot Down Five Houthi Drones Aimed at Asir Region," *Arab News*, June 15, 2019, http://www.arabnews.com/node/1510641/saudi-arabia; "Houthi Drone from Yemen Intercepted as It Targeted Saudi Arabia," *Arab News*, June 27, 2019, http://www.arabnews.com/node/1516686/saudi-arabia; Mina Aldroubi, "Saudi

the world and American-made Patriot missile defense systems, the Houthis' drones have proven capable of penetrating those defense systems and inflicting casualties on various important targets.[202]

The Houthis' weaponized drone program has benefited greatly from the support of Iran, which has supplied them with military-grade drones and an indigenous manufacturing capability beyond what is available to most other VNSAs.[203] Drones recovered from Houthi strikes in southern Saudi Arabia have been identified as Qasef-2Ks or Qasef-1s, capable of travelling up to 90 miles, and nearly identical to the Ababil-T, a drone produced by Iran Aircraft Manufacturing Industries.[204] In late 2018, Houthi forces began to use ISR drones with a range of 900 miles and a top speed of more than 150 miles per hour.[205] On May 14, 2019, a Houthi drone struck Aramco oil stations deep within Saudi Arabia's borders, and well outside the 90-mile limit of Qasef drones, suggesting that the Houthis have successfully adopted longer range drones.[206] As a result, the number of possible targets available to the Houthis has widened. Their target range now seemingly includes almost all of Saudi Arabia, Oman, the U.A.E., Qatar, and Kuwait, with various populous cities potentially in their crosshairs.[207]

Targeted Killings. Another threat that has emerged during the breakthrough period was the potential for VNSAs' drones to be used to carry out assassinations. Advances in imaging technology and reductions in drone size made it possible for VNSAs to identify and target specific individuals. This threat was foreshadowed by the aforementioned 2013 stunt by a member of the German Pirate Party, where a pilot crash-landed a small drone in front of Chancellor Angela Merkel's podium.

Mexican cartels were perhaps the first VNSAs to demonstrate a capability to engage in targeted killings. In July 2018, two drones were spotted in the vicinity of the home of Baja California's *Secretario de Seguridad Pública Estalal* (Public Safety Secretary). One drone provided ISR and command and control capability overhead, while another drone equipped with two fragmentation grenades and a threatening message landed outside the Secretary's door as he was preparing to leave the residence.[208] While the grenades had been rendered inert prior to the mission—making the incident more of a threat than an attack—the plotters were able to deliver a payload effectively and avoid detection or arrest. This incident thus demonstrates the *capability* to use drones in targeted killings.

The threat of targeted killings came to the fore in an August 2018 plot to assassinate Venezuelan president Nicolás Maduro. According to Venezuelan authorities, the plotters used a pair

---

Arabia Intercepts Houthi Drone Headed for the Kingdom," *The National* (U.A.E.), July 1, 2019, https://www.thenational.ae/world/mena/saudi-arabia-intercepts-houthi-drone-heading-for-the-kingdom-1.881531.

[202] See discussion in Jared Malsin, "Iran-Allied Houthis Expose Holes in Saudi Arabia's Missile Defense," *The Wall Street Journal*, June 25, 2019, https://www.wsj.com/articles/iran-allied-houthis-expose-holes-in-saudi-arabias-missile-defense-11561455002.

[203] Dion Nissenbaum & Warren P. Strobel, "Mideast Insurgents Enter the Age of Drone Warfare," *Wall Street Journal*, May 2, 2019.

[204] See "AP Explains: How Yemen's Rebels Increasingly Deploy Drones," *Voice of America*, January 19, 2019, https://www.voanews.com/middle-east/ap-explains-how-yemens-rebels-increasingly-deploy-drones.

[205] Nissenbaum & Strobel, "Mideast Insurgents Enter the Age of Drone Warfare."

[206] "A Saudi Pipeline Attack Amps up Suspicions on the Arabian Peninsula," Stratfor, May 14, 2019.

[207] Ibid.

[208] John P. Sullivan, Robert J. Bunker & David A. Kuhn, "Armed Drone Targets the Baja California Public Safety Secretary's Residence in Tecate, Mexico," *Small Wars Journal*, August 6, 2018, https://smallwarsjournal.com/jrnl/art/mexican-cartel-tactical-note-38-armed-drone-targets-baja-california-public-safety.

of DJI hexacopter drones, each laden with roughly one kilogram of explosives.[209] Due to a combination of countermeasures and apparently poor piloting skills, neither drone made it close enough to Maduro to succeed. One crashed into the side of an apartment building and detonated several blocks away, and the other exploded roughly 100 meters away from him.[210] It remains unclear what group was responsible for the attempt.

A successful VNSA-initiated targeted killing involving drones occurred in January 2019, when several high-ranking members of the Yemeni military, including the head of Yemen's intelligence service and the governor of a province, were assassinated during a military parade. Houthi rebels carried out the attack using an Iranian-designed (and possibly Iranian-manufactured) Ababil-T drone capable of carrying between 70 and 100 kilograms of explosives.[211] It denoted above the dais where a number of VIPs were seated. According to a Houthi spokesman, the drone detonated after "accurate surveillance of the enemy commanders' movements."[212] This attack was successful, at least in part, due to the Houthis' access to advanced weapons systems provided by Iran. However, the attack should also be seen as a proof of concept for other VNSAs, and more attacks like it are likely.

Smuggling. The breakthrough period also saw rapid proliferation in groups seeking to use UASs to transport illicit material, as criminal VNSAs took advantage of drones that could fly farther and faster, and carry a heavier payload. Early drones like the DJI Phantom were not designed to carry a payload: The amount of weight they could be retrofitted to carry was less than one kilogram. But newer platforms like the DJI Matice are built to carry payloads of up to six kilograms.[213] While drones like the Matice are more expensive, the economic advantages of smuggling with a more capable drone are clear.

In addition to improvements in off-the-shelf systems, the breakthrough period saw cartels begin designing and building their own drones using commercially available parts at a cost that made drones more attractive in some instances than tunnels or semi-submersibles.[214] At the U.S.-Mexico border, there was a marked increase in the frequency of drones crossing into the United States while carrying drugs. While there is no concrete open-source data on the increase, reporting suggests that drone use for these purposes may have quadrupled between 2017 and 2018.[215] More recently, in April 2019, a drone was used as a scout to reconnoiter potential routes for smuggling people into the United States.[216] Similar developments have occurred in Europe, particularly Ukraine, where drones are used

---

[209] Nick Waters, "Did Drones Attack Maduro in Caracas?," *Bellingcat*, August 7, 2018, https://www.bellingcat.com/news/americas/2018/08/07/drones-attack-maduro-caracas/.
[210] Christoph Koettl & Barbara Marcolini, "A Closer Look at the Drone Attack on Maduro in Venezuela," *The New York Times*, August 10, 2018, https://www.nytimes.com/2018/08/10/world/americas/venezuela-video-analysis.html?login=email&auth=login-email.
[211] Mohammed al-Kibsi, "Houthi Drone Targets Senior Yemeni Officers, Kills Five Soldiers," *Al-Jazeera*, January 10, 2019.
[212] Ibid.
[213] DJI, "Matice 600 Specs," https://www.dji.com/ca/matrice600/info#downloads.
[214] "Carteles Hacen Drones para Trasiego Hacia EU," *La Cronica* (Mexico), July 10, 2014.
[215] Gina Harkins, "Drone Drug Flights Surge Along U.S.-Mexico Border as Smugglers Hunt for Soft Spots," *National Post*, June 25, 2018, https://nationalpost.com/news/world/secret-drone-flights-surge-along-u-s-mexico-border-as-smugglers-hunt-for-soft-spots.
[216] Daniel Borunda, "Border Patrol: Smugglers Fly Drone Scout Over Border in New Tactic in El Paso Region," *El Paso Times*, April 17, 2019, https://www.elpasotimes.com/story/news/immigration/2019/04/17/drone-over-border-flown-smugglers-filmed-border-patrol-el-paso/3502381002/.

to move goods (primarily tobacco) across borders.[217]

Prison smugglers have also made use of drones, with smuggling rings disrupted across Europe and North America, including in Ontario and Quebec.[218] To date, most of the disrupted networks have been smuggling such contraband as cell phones, drugs, and tobacco. There is at least one case of a drone being used to smuggle in a pair of wire cutters that helped inmates escape from a maximum security prison in South Carolina.[219] Another prison-related use of drones was a prison break in France that involved several drone flights around the prison to identify its vulnerabilities. The reconnaissance eventually identified a recreation yard that lacked anti-aircraft netting, which subsequently allowed a helicopter to land, and one of France's most notorious criminals to escape.[220]

Proliferation of Other Unmanned Platforms. While UAS have been the most prolific example of unmanned systems being employed by VNSAs, these actors have also employed other unmanned platforms, including remote-controlled boats and vehicles. Remote-controlled VBIEDs have seen limited use in Libya and Iraq. While not particularly hard to manufacture, remote-controlled full-size vehicles are difficult to maneuver remotely. One analyst who tracks VBIEDs has identified only one instance of Daesh successfully using a remote-controlled VBIED in Iraq, while another Daesh-built remote-controlled VBIED was captured in Libya.[221] In some ways, VNSAs' use of this technology mirrors where UASs were roughly 10 years ago: VNSAs are experimenting with, and iterating on, this technology, but are not yet at the point where commercially-available technology has made these operations feasible or economic.

Where VNSAs' breakthrough in their use of other unmanned platforms has occurred is in the weaponization of small boats by Yemen's Houthi rebels—again, likely with significant Iranian support. Beginning in 2017, a number of successful and attempted attacks struck Saudi navy vessels and a Saudi oil terminal using boats that had been retrofitted to work via remote control.[222] The tactic of using a water-borne IED is itself not new—it was used, for example, in al-Qaeda's attack on the U.S.S. *Cole* in Yemen in 2000—but remote-piloted boats represent an emergent threat.[223]

---

[217] Marco Margaritoff, "Tobacco-Smuggling Drone Found by Ukraine Border Patrol Reveals Region's Black Market," *The Drive*, September 7, 2018, https://www.thedrive.com/tech/23447/tobacco-smuggling-drone-found-by-ukraine-border-patrol-reveals-regions-black-market.

[218] "'Well-Organised' Gang Flew Drones Carrying Drugs into Prisons," *BBC*, August 30, 2018, https://www.bbc.com/news/uk-england-45358876; Darry Davis, "Correction Officials Raise Concerns Over Drone Smuggling Contraband into Kingston-Area Prisons," *Global News*, March 20, 2019, https://globalnews.ca/news/5074018/drones-smuggling-contraband-into-prisons-kingston/.

[219] Eric Levenson & Sheena Jones, "South Carolina Inmate Used Drone, Makeshift Dummy to Escape Prison," *CNN*, July 7, 2017, https://www.cnn.com/2017/07/07/us/sc-prison-escape-drone/index.html.

[220] David Chazan, "Drones Over Prison May Have Been Reconnaissance Mission for French Gangster's Prison Break," *The Telegraph* (UK), July 2, 2018, https://www.telegraph.co.uk/news/2018/07/02/drones-prison-may-have-reconnaissance-mission-french-gangsters/.

[221] See Hugo Kaaman (@HKaaman), tweet, January 5, 2019 (noting that "There's only 1 RC-VBIED by IS ever recorded on footage (Ninawa/Dec, 2015)"); Hugo Kaaman, "The SVBIEDs of the Islamic State in Libya—History & Analysis," blog entry, February 5, 2019, https://hugokaaman.com/2019/02/05/the-svbieds-of-the-islamic-state-in-libya-history-analysis/.

[222] Rosie Perper, "Drone Boats Filled with Explosives Are the New Weapon in Global Terrorism," *Business Insider*, October 4, 2018, https://www.businessinsider.com/drone-boats-filled-with-explosives-houthis-saudi-arabia-2018-10.

[223] Conflict Armament Research was able to investigate a version of the boat that the United Arab Emirates seized. The organization's analysis is worth reading. Conflict Armament Research, *Anatomy of a 'Drone Boat'* (London: Conflict Armament Research, December 2017), www.conflictarm.com/download-file/?report_id=2550&file_id=2564.

Competition

For most of the past two decades, Western countries, and the United States in particular, have enjoyed a near-monopoly on technologically advanced unmanned systems, and airspace in general. In the late 2000s, analysts increasingly raised the prospect of VNSAs using drone technology.[224] But, as this report details, many early plots appeared to be fantastical rather than serious threats. Counter-drone technology aimed at smaller, less-expensive platforms was not a priority. Indeed, the need for serious counter-drone technologies only became clear with the rapid advance of drone technology itself.

In the breakthrough period, VNSAs moved rapidly from ineffective plots to tactically sophisticated ISR and attacks. As a result, a multitude of counter-drone systems have emerged. A 2018 report by the Center for the Study of the Drone at Bard College identified 155 manufacturers that now produce 235 distinct counter-drone systems (for both detection and interdiction) employing a variety of technologies: electronic jamming, acoustic detection, using nets to entangle drone rotors, lasers, and machine guns.[225]

Despite the rapid growth in this industry, drones still appear to have the upper hand as a threat. As one example, a series of drone sightings around London's Gatwick—almost certainly a malicious use of UAS, but seemingly a non-terrorist one—caused the airport to close for 36 hours during the peak of holiday travel season in late 2018. British law enforcement was unable to obtain the necessary approvals to use a counter-drone system intended for the military in that setting.[226]

Following the incident at Gatwick, DJI updated its geofencing software to create three dimensional "no-fly" zones around a series of European airports and sensitive facilities.[227] The company has rapidly expanded its geofencing program, which was expanded to cover large swaths of Syria and Iraq in 2017 after Daesh's use of weaponized DJI drones came to light.[228] But these countermeasures can be defeated by a skilled VNSA through the process of manually overriding the geofencing. Demonstrating this, within months of DJI's geofencing in Syria and Iraq, a group of Russian hackers calling themselves "Coptersafe" released a hack to get around the restrictions for only $200 per device (and, in turn, DIY hackers later "reverse-engineered the Coptersafe software and … released it for free" on the Internet).[229] After DJI fixed this vulnerability, drone pilots took to social media to work together on finding additional workarounds, citing concerns over DJI's ability to exert too much control over its products after they were sold.[230] This divide between consumers and

---

[224] See, for example, Brian A. Jackson et al., *Evaluating Novel Threats to the Homeland: Unmanned Aerial Vehicles and Cruise Missiles* (Santa Monica, CA: The RAND Corporation, 2008), https://www.rand.org/pubs/monographs/MG626.html.

[225] Arthur Holland Michel, *Counter-Drone Systems* (Annandale-on-Hudson, NY: Center for the Study of the Drone at Bard College, 2018), pp. 2, 4, http://dronecenter.bard.edu/counter-drone-systems/.

[226] Heather Farmgrough, "Gatwick Fiasco Puts Anti-Drone Technology Under the Radar," *Forbes*, December 31, 2018, https://www.forbes.com/sites/heatherfarmbrough/2018/12/31/gatwick-fiasco-puts-anti-drone-technology-on-the-radar/#2279ecac7708.

[227] DJI Technology, press release, "DJI Improves Geofencing to Enhance Protection of European Airports and Facilities," February 12, 2019, https://www.dji.com/ca/newsroom/news/dji-improves-geofencing-to-enhance-protection-of-european-airports-and-facilities.

[228] Gareth Corfield, "Drone Maker DJI Quietly Made Large Chunks of Iraq, Syria No-Fly Zones," *The Register* (U.K.), April 26, 2017, https://www.theregister.co.uk/2017/04/26/dji_drone_geofencing_iraq_syria/.

[229] Ben Sullivan, "DJI is Locking Down Its Drones Against a Growing Army of DIY Hackers," *Vice News*, July 7, 2017, https://www.vice.com/en_us/article/3knkgn/dji-is-locking-down-its-drones-against-a-growing-army-of-diy-hackers.

[230] Ibid.

manufacturers—and frustrated consumers' subsequent search for technical workarounds—is one that VNSAs will be capable of exploiting.

Future Violent Non-State Actor Adoption of Technology

As this study's adoption curve shows, as current technologies improve and new technologies are developed, VNSAs will continually seek to incorporate these tools into their arsenals. As our discussion of VNSAs' use of social media and UAS technology shows, the incorporation of these new technologies will not be instantaneous, nor will it be smooth. There is also no guarantee that it will be successful.

VNSAs will continue to engage in DIY (do-it-yourself) innovation. Incremental improvements to existing technologies may allow groups to customize those technologies. This was the case with drones. A store-bought quadcopter did not come with a bomb bay, but through clever engineering, Daesh was able to attach an explosive delivery system and turn the quadcopter into a lethal weapon.

While DIY innovation will continue to play an important role in VNSA technological adoption, there will likely be some advances that remain too complex for VNSAs to replicate on their own. For example, even though VNSAs would likely benefit from increasing the speed, range, and maneuverability of drones, it is unlikely that a VNSA will have the technical expertise to build jet-propelled drones (though a VNSA with a large-scale technical operation, such as that of Aum Shinrikyo that this study previously described, may be able to do so). The innovations of private commercial firms will therefore remain a crucial driver of VNSA adoption of new technologies.

While VNSAs will seek to incorporate many different technologies as they become available, this section focuses in particular on drones, artificial intelligence, and cryptocurrency, which we believe to be worthy of particular interest.

Future VNSA Drone Uses

As we have shown, VNSAs have used drones for various purposes over the past several years, and in doing so introduced a new set of threats against which state actors must be prepared. There have been significant developments in drone technology that allow drones to fly farther, faster, carry heavier payloads, and mount various tools and weapons. And further UAS developments that may benefit VNSAs are on the horizon. This section examines potential future tactical uses of drones, then details the technological developments that will be particularly relevant to VNSAs

Tactical Applications of Drones for VNSAs.

Swarms. Drone swarms provide numerous tactical advantages. If a VNSA lacks drones that can carry heavy weapons, swarms may be employed to increase the volume of ordnance. Drone swarms would ideally operate with AI technology that allows individual drones to communicate with one another and adapt to the battlefield. The AI could also enable drones to make specific targeting decisions, such as the identification of high-priority over low-priority targets, or identifying and disabling enemy communications systems.[231] Such technology would effectively transform the drones

[231] See discussion in Kyle Mizokami, "The U.K. Promises to Develop Drome Swarms, but on an Unrealistic Timetable," *Popular Mechanics*, February 12, 2019, https://www.popularmechanics.com/military/research/a26307975/uk-drone-swarms/.

from inanimate weapons to sentient soldiers, thereby strengthening the resiliency of attacks. The development of algorithms to facilitate intelligent drone swarms is being actively pursued by states for military and civilian applications.[232] As has been the case in other areas, commercialization may provide a myriad of applications that VNSAs will be able to acquire, replicate, or adapt.

Incorporation into Complex Attacks. Drones can also be used in larger, more complex attacks. One such use is resource re-supply, where drones would bring ammunition, weapons, food, or other supplies to fighters. This would eliminate the need to carry resources or store them beforehand, saving valuable time and energy.[233] VNSAs have previously needed to find creative solutions to ensure resource access, as demonstrated in the 2013 Westgate Mall attack in Nairobi. Weeks before the shooting, the attackers rented a shop space with fraudulent identification—an expensive and time-consuming endeavor—to cache weapons and other resources.[234] While the payload of commercially-available drones is currently limited (though not as much as it used to be), the arc of UAS developments suggests that commercially-available drones' payload will grow, perhaps to the point that remote re-supply will become practical for VNSAs.

Another use that VNSAs may put drones to in complex attacks is using miniature drones to gain access to buildings or smaller areas. Very small drones capable of streaming video to a cellphone or wrist-mounted monitor, operating in GPS-denied areas, and operating on frequencies that are more challenging to jam would be very useful for reconnaissance in areas with limited human access.[235] Miniaturized drones may also be equipped with AI technology (which we discussed further subsequently) to enable targeted, and perhaps untraceable, assassinations.[236]

Drone Technologies Likely to be Exploited by VNSAs.

We now explore several specific technologies that we judge VNSAs likely to exploit with respect to drones over the next five years.

Heavy Lift Drones. The payload that commercially available drones can carry has increased steadily, as has their maximum flying time with heavier payloads. The ability to carry heavier loads for longer distances will benefit VNSAs that rely on drones to transport material, whether it is an explosive device, combat resources, or drugs. These technological improvements will also help VNSAs to avoid the detection they may risk with human transports and vehicle convoys.

Chemical Dispersion. VNSAs have long been eager to use drones for the delivery of CBRN weapons. This has so far been stymied by their inability to develop an effective dispersal system. Due

---

[232] See Clayton Schuety & Lucas Will, "An Air Force 'Way of the Swarm': Using Wargaming and Artificial Intelligence to Train Drones," *War on the Rocks*, September 21, 2018, https://warontherocks.com/2018/09/an-air-force-way-of-swarm-using-wargaming-and-artificial-intelligence-to-train-drones/; Randy Rieland, "Teaching Drones to Sniff Out Toxic Air," *Smithsonian Magazine*, September 11, 2018, https://www.smithsonianmag.com/innovation/teaching-drones-sniff-out-toxic-air-180970231/.

[233] "How Autonomous Delivery Drones Could Revolutionise Military Logistics," *Army Technology,* October 8, 2018, https://www.army-technology.com/features/autonomous-delivery-drones-military-logistics/.

[234] "Terrorists Rented Shop, set up Al-Shabab Base in Kenyan Mall Before Slaughtering Dozens: Report," Associated Press, September 27, 2013, https://nationalpost.com/news/kenya-terrorists-rented-shop-in-the-mall-reports.

[235] See discussion in Jim Aloisi, "Send in a Drone First," Strax Intelligence Group, May 24, 2018, http://straxintelligence.com/send-in-a-drone-first.

[236] See discussion in Max Tegmark, *Life 3.0: Being Human in the Age of Artificial Intelligence* (New York: Penguin, 2018).

to improvements in chemical dispersion technology, however, some state actors have successfully modified commercial drones to deploy CBRN weapons like tear gas.[237] VNSAs could potentially replicate this technique.

Recently, drones with liquid dispersion capabilities have been developed for agricultural purposes.[238] One early model, released by DJI, can carry up to 10kg of liquid. Most VNSAs would consider these models extremely expensive, but the prices are likely to fall, as they have done in other technological spheres.

Improvement in Sensors. Rapidly developing technology in the quality and diversity of drone sensors will undoubtedly improve VNSAs' ISR capabilities. Sensors like Light Detection and Ranging (LIDAR), FLIR, or true night vision will allow VNSAs to improve their imaging. Potential uses include pre-attack reconnaissance and improving smuggling routes. Such tools could potentially act as replacements for human surveillance, with their ability to surveil undetected for longer periods of time, potentially utilizing facial recognition software. The price of advanced sensors is falling rapidly at present.

Horizontal Proliferation of Remote-Controlled and Autonomous Technology. While VNSAs have historically made some use of remote-controlled vehicles, limits in maneuverability and complicated controls have impeded their adoption. Some companies have recently demonstrated significant progress on heavier remote-controlled commercial vehicles, advances that could potentially be applied to passenger vehicles as well.[239] Developments in this technology present possibilities for VNSAs, which may use remote-controlled cars for VBIED attacks, car ramming attacks, or resource transportation/smuggling. Parallel to this innovation is the developing industry of self-driving cars, which could offer similar possibilities.[240] Cartels in particular may also move to develop autonomous submersibles. This has long been discussed as a possibility by observers, but has yet to be seen in practice.[241] Here too military investment in these technologies may have commercial spillovers that make the technology more accessible to VNSAs.

Fixed-Wing Drones. While quadcopter drones have been the primary design used by most VNSAs, fixed-wing drones can fly farther and faster. Fixed-wing drones have generally remained in a higher-end commercial market: They are more expensive and require professional operability, as well as long runways for take-off. Additionally, prohibitions on operating drones Beyond Visual Line of Sight (BVLOS) in many countries could inhibit fixed-wing drones from expanding into the hobbyist

---

[237] Drones have been prominently employed in this manner by the Israel Defense Forces. Nick Waters describes the dispersal of tear gas against protesters as "by far the most prominent and controversial IDF use of commercial drones." Nick Waters, "First ISIS, Then Iraq, Now Israel: IDF Use of Commercial Drones," *Bellingcat,* June 18, 2018, https://www.bellingcat.com/news/mena/2018/06/18/first-isis-iraq-now-israel-idf-use-commercial-drones/.

[238] DJI, press release, "DJI Introduces Company's First Agricultural Drone," November 27, 2015, https://www.dji.com/ca/newsroom/news/dji-introduces-company-s-first-agriculture-drone.

[239] See discussion in Ira Boudway, "With Driverless Cars Running Late, a Startup Tries Remote-Control Trucks," Bloomberg, April 18, 2019, https://www.bloomberg.com/news/articles/2019-04-18/phantom-auto-expands-remote-driving-to-trucks-forklifts.

[240] See discussion in James Black, "Autonomous Vehicles: Terrorist Threat or Security Opportunity?," The RAND Corporation, January 3, 2018, https://www.rand.org/blog/2018/01/autonomous-vehicles-terrorist-threat-or-security-opportunity.html.

[241] See discussion in Danielle Muoio, "Here's All the High-Tech Gear Cartels Use to Sneak Drugs into the US," *Business Insider*, July 20, 2016, https://www.businessinsider.com/cartels-use-tech-to-sneak-drugs-into-the-us-2016-7 (quoting Marc Goodman).

market. However, both Daesh and also some cartels have shown evidence of researching and developing their own fixed-wing drone technology.[242] The drones used in the Khmeimim airbase attack were rudimentary fixed-wing models.

Breakthroughs in Easier to Use Commercial Components. The Khmeimim drone swarm illustrated yet another development in drone technology: the proliferation of simpler and higher-quality components for constructing custom devices.[243] Though many parts of the Khmeimim attack drones were jerry-rigged and built by hand, they also incorporated customizable components, including a bomblet release mechanism. Rather than purchasing expensive models, some VNSAs will opt for in-house manufacturing by using relatively cheap and high-quality components. This is already observable for some cartel uses.[244]

Future VNSA Uses of Artificial Intelligence

Many of the artificial intelligence (AI) systems that VNSAs could deploy already exist, but are not yet widely available to consumers. But similar to drones, VNSAs are likely to adopt AI systems as they become more accessible and easier to use for consumers in general. AI has the potential to improve all aspects of VNSA activity, including recruitment, fundraising, ISR, and attacks.

We have identified two primary criteria likely to have an impact on whether VNSAs will adopt different AI systems in the near term (next five years). First, is the AI system commercially available, cheap, and easy to use, or will it be in the next five years? Second, would it fit into strategies, planning structures, and recruitment tactics currently employed by VNSAs? AI systems that we evaluate to be *likely* to be adopted by VNSAs in the next five years are easily accessible to general audiences and fit into current strategies. To be clear, likely adoption does not mean likely success: Per the adoption curve that this study introduces, initial uses may look like failures, and VNSAs may never succeed in reaching the breakthrough phase. AI systems that are *possible* to be adopted in the next five years are less accessible (*e.g.*, harder for untrained people to use, more expensive), or they don't fit into current VNSA goals or strategies. We now examine, in turn, AI systems that are *likely* to be adopted by VNSAs in the next five years, and then those that *may* be adopted, but that we do not necessarily judge more likely than not.

AI Systems Likely to be Adopted by VNSAs in the Next Five Years

Deep Fakes. Deep fake technology can alter videos, images, or voice recordings to create fake content that appears strikingly real. This is achieved by providing photographs, videos, and audio recordings of a specific person to an advanced machine-learning algorithm, which in turn generates a nearly identical appearance and voice. Typically, this algorithm will refine its creation by checking it against another algorithm intended to detect fraudulent videos or recordings. Once the fraud checker no longer indicates that the content is fake, the original algorithm concludes that it has successfully

[242] See discussion in Rassler, Al-'Ubaydi & Mironova, *The Islamic State's Drone Documents*; "Descubren un 'Narcodron' en Colombia; Enviaba Cocaína a Panamá," *Excelsior* (Mexico), November 16, 2016.
[243] See discussion in Mark Jacobsen, "Why the Flying IED Threat Has Barely Started," *War on the Rocks,* October 19, 2016, https://warontherocks.com/2016/10/why-the-flying-ied-threat-has-barely-started/.
[244] See discussion in "Carteles Hacen Drones para Trasiego hacia EU," *La Cronica* (Mexico), July 10, 2014.

created a functioning deep fake.[245] This means that to the human eye, it will often be nearly impossible to detect a deep fake.[246]

Deep fakes prey on the notion that seeing—or hearing—is believing, as they are designed to trick individuals into believing that their fabricated content is legitimate.[247] Thus far, deep fakes have been used in contexts that include pornography and political mudslinging. In the context of pornography, some existing deep fake videos convincingly place the likenesses of famous actresses, and other famous women, into pornographic scenes. Those victimized include movie stars Natalie Portman, Emma Watson, and Gal Gadot—and in the context of famous women who are not actresses, Michelle Obama, Ivanka Trump and Kate Middleton.[248] As the technology improves, the list of deep fakes' potential uses in all contexts—crude or otherwise—is nearly endless.

Deep faking apps are readily available even now. They are typically cheap, or free.[249] FakeApp, the most popular deep fake app for Windows operating systems, is free to download and free to use. Users may buy computer hardware to improve the functionality of FakeApp, but it appears that standard computer components will support the program. There are also numerous online tutorials for FakeApp. Aspiring deep fakers can watch YouTube videos, or find written guides, explaining how to create a fabricated image from start to finish.[250]

All of this raises the possibility of VNSAs using deep fake AI systems to create content that can serve their purposes. For example, Daesh or VNSAs with a similar ideology could create fabricated videos depicting Western forces desecrating the Qur'an. For an example of how this can inflame passions that might advances VNSAs' goals, one need look no further than March 2011, when riots erupted in Afghanistan after an obscure American clergyman at a small Florida church posted a video online in which he burnt a Qur'an. Rioters in Mazar-i-Sharif killed seven United Nations staff members.[251] Similarly, extreme right-wing or left-wing VNSAs may employ deep fakes of political figures to advance conspiracy theories that serve their causes. For example, right-wing extremists seeking to incite anti-Semitic fervor could fabricate video of George W. Bush and former Israeli prime minister Ariel Sharon planning the 9/11 attacks. The creative, and nefarious, possibilities are virtually limitless.

---

[245] See discussion in J.M. Porup, "How and Why Deepfake Videos Work – And What is at Risk," *CSO Online*, April 10, 2019, https://www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html.

[246] Here is a video demonstrating the versatility, verisimilitude, and potential of deep fakes: https://www.youtube.com/watch?v=T76bK2t2r8g.

[247] As deep fakes grow in popularity, individuals are likely to increasingly question the veracity of legitimate images, videos, and recordings, further eroding public confidence in what is real and true. John Villasenor, "Artificial Intelligence, Deepfakes, and the Uncertain Future of Truth," The Brookings Institution, February 14, 2019, https://www.brookings.edu/blog/techtank/2019/02/14/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth/.

[248] Dave Lee, "Deepfakes Porn Has Serious Consequences," *BBC*, February 3, 2018, https://www.bbc.com/news/technology-42912529.

[249] Examples of free online software options for deep-faking include https://deepfakesapp.online and https://github.com/iperov/DeepFaceLab.

[250] Here is an example of a YouTube tutorial on deep-faking: https://www.youtube.com/watch?v=wBax7_UWXvc. For a written tutorial on deep fakes, see Alan Zucconi, "How to Install Fake App," blog entry, March 14, 2018, https://www.alanzucconi.com/2018/03/14/how-to-install-fakeapp/.

[251] "Riots in Afghanistan Follow Fla. Quran Burning," *NPR*, April 2, 2011, https://www.npr.org/2011/04/02/135063155/violence-in-afghanistan-after-quran-burned-in-u-s.

For now, only relatively high-profile individuals—or aspiring YouTube stars who have copious amounts of video of themselves available online—are likely to be subjected to deep fakes. Deep fakes require many images or recordings of the target one wants to depict. But imaginative VNSAs could create powerful videos even with a limited pool of deep fake candidates. Additionally, as deep fake technology improves, and as normal people continue to post more images and videos of themselves on the web, VNSAs may also be able to target ordinary citizens with deep fakes.

Virtual Agents. Virtual agents, also known as "chatbots," are AI programs that mimic human interactions over text. They have been used in various ways, perhaps most commonly as a mechanism to answer questions or provide information to someone viewing a website. For example, a user who sends an instant message to a company offering 24/7 chat-based customer support may be interacting with a chatbot. Chatbots can also be used in other contexts, such as taking food or grocery orders. Starbucks and Whole Foods are among the major brands experimenting with chatbots.[252]

Two uses of virtual agent technology potentially of relevance to VNSAs are the creation of social media chatbots and the development of recruitbots. VNSAs that rely on a toxic discursive environment may be able to create their own chatbots to post inflammatory content without human intervention. For ideological VNSAs, this could prove useful in creating an extremist or bigoted milieu—or alternatively, because it may help to polarize and radicalize their *opponents*. Such use of chatbots would also increase the likelihood of their topics trending on social media.[253]

Virtual agent technology has also been used to create "recruitbots," which can help employers to identify ideal candidates for employment.[254] It is possible that a tech-savvy VNSA could eventually repurpose such technology to identify potential recruits, or even initiate the recruitment process (for example, for terrorist operatives or people involved in illicit commerce).[255] Recruitbots could expand the potential pool of VNSA recruits and also help to shield VNSAs' human recruiters from possible arrest.

Virtual agent technology is already widely available on the Internet. For example, people can now create chatbots in "a few minutes" through a company called Dexter.[256] The company allows people to build the bots for free: They only pay if the bots are able to attract users. Even then, the bots are not expensive: A bot able to accommodate simultaneous chats with 5,000 users costs only $80 per month.[257] At the same time, recruitbots are not yet capable of performing the full range of tasks that a human recruiter would. Nonetheless, as VNSAs pursue innovative ways to produce content and interact with recruits, and as virtual agent technology continues to improve, it is highly likely that VNSAs will incorporate virtual agents into their arsenals.

---

[252] Todd Wasserman, "Chatbots Are All the Rage—and Something of a Risk," *Security Roundtable*, March 21, 2018, https://www.securityroundtable.org/chatbots-rage-something-risk/?doing_wp_cron=1555957875.3937430381774902343750.

[253] Compare discussion in J.M. Berger & Jonathon Morgan, *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter* (Washington, DC: The Brookings Institution, 2015), p. 29, https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.

[254] Here is an example: https://www.therecruitbot.com.

[255] See discussion in Len Epp, "Five Potential Malicious Uses for Chatbots," *Medium*, May 10, 2016, https://medium.com/@lenepp/five-potential-malicious-uses-for-chatbots-a15f4955fba7.

[256] Wasserman, "Chatbots Are All the Rage."

[257] Dexter, "Pricing," n.d., https://rundexter.com/pricing/ (accessed July 5, 2019).

AI Systems That May be Adopted by VNSAs in the Next Five Years

Social Network Mapping & Analysis. Social network mapping software allows users to analyze social networks and identify communities, influencers, platforms, and demographics of users in online networks. Even for individuals who attempt to extricate themselves from web-based social networks, "data inference" can provide insights into one's interests, habits, and social circles.[258] Coupled with machine-learning algorithms that can identify trends and linkages within and between one's social networks, collecting information on users (or for VNSAs, potential targets and recruits) is becoming increasingly effective and efficient.

Social network mapping can also show individuals' importance in a social network. For typical civilian purposes, this might indicate to a brand that they should offer a sponsorship deal to a certain individual, given that person's influence over a desired demographic. For VNSAs, social network mapping may inform targeting preferences. For example, an organized criminal group may use social network mapping to determine who to target in a rival group to extract concessions or debilitate the group. An insurgent VNSA may use social network mapping to figure out how to conquer a city.

The idea of VNSAs conducting social network analysis is not new, and in fact there are demonstrated instances of this occurring. But until now, it has been done manually. For example, Daesh relied on human intelligence to map the social landscape of territory it sought to conquer in Syria and Iraq, as well as in Ben Guerdane, Tunisia. It is well documented that the group's early battlefield victories in the Syria-Iraq theater were enabled, in part, by ex-Baathist intelligence operatives who mapped cities' key players and power brokers, monitored their pattern of life, and helped Daesh to kill or imprison them. Similarly, when North African Daesh operatives attacked the Tunisian town of Ben Guerdane in March 2016, the available evidence—including the efficient way they assassinated key security officials—suggested that the militants had similarly worked to learn the human terrain in advance. VNSAs may soon be able to use software that conducts this analysis for them at fractions of both the cost and the time that it previously took.

Social network mapping software may also prove valuable in identifying lucrative or vulnerable targets. For example, a group engaging in kidnapping for ransom may be able to analyze a target's social network to infer not only their net worth, but also the net worth—and willingness to pay—of those who might be paying the target's ransom.[259] Analysis of the target's friends, family and colleagues would put them at risk as well. Advanced social network analysis may also allow VNSAs to identify individual vulnerabilities that can be exploited for blackmail or extortion.

AI-enhanced social network analysis software currently exists, though it appears to be reserved largely for well-resourced tech companies. Among other things, these companies rely on AI to analyze users' interests and purchasing patterns, using this information to target ads or content toward them. Though it is difficult to predict when this technology will diffuse into the mainstream, it is likely that it will, and VNSAs will be primed to adopt it.

---

[258] See discussion in Zeynep Tufecki, "Think you're Discreet Online? Think Again," *The New York Times*, April 21, 2019, https://www.nytimes.com/2019/04/21/opinion/computational-inference.html.

[259] Miles Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (Oxford, UK: Future of Humanity Institute, University of Oxford, 2018), p. 26, https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf.

Voice-Enabled AI & Automated Social Engineering. AI deep learning techniques are already being used in telemarketing to mimic human communication patterns, tricking people into believing they are speaking with an actual person rather than a robot.[260] Robocalls may now introduce themselves, hesitate between words or phrases, or respond to verbal cues from the potential customer. The magazine *Inc.* has reported on Google CEO Sundar Pichai demonstrating how the company's Google Assistant can make phone calls in which it successfully mimics a human:

> Pichai showed a demo of the Assistant bot calling a hair salon and impersonating a human, then repeated the same trick by having the bot call a restaurant (it was all pre-recorded). One robot calling one human, booking an appointment, but the human was blissfully unaware of the artificial intelligence at work. Nice. Google samples human voices and then extrapolates what to say during everyday conversations.
>
> The robot even says "um."[261]

While AI cannot yet hold a deep conversation, the topics it can cover, and the fluidity with which it can cover them, will continue to improve. AI voice technology can also, quite obviously, be used for malicious purposes. For example, deep learning techniques can generate custom communications that manipulate people into responding to personal questions, revealing information about people they know, or falling for a scam.[262] This may be achieved, for example, by integrating social network analysis into the virtual agent's arsenal. Should parents post publicly about their children, the virtual agent could autonomously learn about the child, eventually gathering enough information to manipulate the parent into paying money for anything from an overdue library book to bail. These uses fall under the broader umbrella of social engineering, defined by the Office of the Privacy Commissioner of Canada as "the art or practice of manipulating people in order to obtain confidential or sensitive data."[263]

VNSAs have already integrated social engineering into their arsenals. Hamas operatives have posed as women on social media sites in an attempt to contact Israeli soldiers. Adopting Hebrew names and setting their profile pictures to images of conventionally attractive women, the operatives sought to trick the soldiers into downloading software that would allow Hamas to spy or remotely control the soldiers' phones.[264]

With tech behemoths such as Google still in the early stages of developing voice-enabled AI, it is unlikely that VNSAs will be able to adopt this technology in the next five years. Well-resourced VNSAs are likely to be the first adopters of this technology when its time does come. Continued

---

[260] "How Artificial Intelligence has Helped Robocall Technology Evolve," Technology.org, January 31, 2018, https://www.technology.org/2019/01/31/how-artificial-intelligence-has-helped-robocall-technology-evolve/.
[261] John Brandon, "This Is the Worst Use of Artificial Intelligence You Will Read About All Day. Thank You So Much, Google," *Inc.,* May 9, 2018, https://www.inc.com/john-brandon/this-is-worst-use-of-artificial-intelligence-you-will-read-about-all-day-thank-you-so-much-google.html.
[262] John Markoff, "As Artificial Intelligence Evolves, So Does Its Criminal Potential," *The New York Times*, October 23, 2016, https://www.nytimes.com/2016/10/24/technology/artificial-intelligence-evolves-with-its-criminal-potential.html.
[263] Office of the Privacy Commissioner of Canada, "Recognizing Threats to Personal Data Online," March 2007, https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/online-privacy/phishing/.
[264] Judah Ari Gross, "After Facebook, Hamas Turns to Instagram to Lure IDF Soldiers, Army Says," *Times of Israel*, August 15, 2018, https://www.timesofisrael.com/after-facebook-hamas-turns-to-instagram-to-lure-idf-soldiers-army-says/.

improvements in AI's ability to mimic human interaction—vocally or otherwise—raises the threat of increasingly frequent and sophisticated social engineering attacks.

Person & Object Recognition Software. Computerized person and object recognition continues to improve. At its core, this process involves scanning an image to catalogue individual pixels and the relationships between them, and comparing these markers to other images of a unique person or object to determine whether they are a match. If they match, the software can then alert interested parties, or track those pixels across multiple images in real time. This basic process has been used for years by a number of actors, ranging from law enforcement to casinos.[265] With deep learning, the accuracy and speed of person and object recognition has only grown.

For VNSAs, the ability to remotely identify and track individuals or objects provides multiple potential benefits. With respect to ISR, VNSAs could program static or vehicle-mounted cameras to provide real-time updates on the whereabouts of adversarial actors. This could allow them to track assassination or kidnapping targets, and to identify informants speaking to authorities. It could also be of use to criminal groups that seek to hide their activities from authorities. By using object recognition software as their "lookouts," these groups could become increasingly difficult to track and interdict. Beyond ISR, person and object recognition software can be used to enhance weapons systems—for example, by programming drones with visual recognition software to automatically track targets.[266] These drones could lock on to individuals to carry out assassinations, or they could lock on to objects to serve as detonators for larger attacks.[267]

The widespread adoption of person and object recognition software is still largely reserved for well-resourced organizations. This is partially because it requires a robust network of cameras and significant computing power to provide accurate, comprehensive insights.

Future VNSA Uses of Cryptocurrency

VNSAs may increase their use of cryptocurrencies to anonymously procure goods and services, pay personnel, and improve operational efficiency.[268] Of the current total market value of cryptocurrencies, illicit use represents only a small percentage of transactions. Likewise, of VNSAs' total economic activity, the scale of cryptocurrency use pales in comparison to traditional methods of illicit finance.[269] But the rapidly evolving nature of cryptocurrency platforms, including trends toward increased anonymization, suggests the potential for cryptocurrencies to become a more important tool for VNSAs.

---

[265] Brad Chacos, "7 Casino Technologies They Don't Want You to Know About," *Gizmodo*, August 10, 2011, https://www.gizmodo.com.au/2011/08/7-casino-technologies-they-dont-want-you-to-know-about/.

[266] See discussion in Norman Di Palo, "How to Add Person Tracking to a Drone Using Deep Learning and NanoNets," *Medium*, June 21, 2018, https://medium.com/nanonets/how-i-built-a-self-flying-drone-to-track-people-in-under-50-lines-of-code-7485de7f828e.

[267] T.X. Hammes, "Technology Converges; Non-State Actors Benefit," The Hoover Institution, February 25, 2019, https://www.hoover.org/research/technology-converges-non-state-actors-benefit.

[268] As will be discussed in this section, most cryptocurrencies are best understood as pseudonymous rather than anonymous in nature. However, we refer to the relevant attribute of cryptocurrencies as *anonymity* in this sentence because that is precisely what VNSAs who choose to utilize cryptocurrencies hope they will provide, by obscuring the actors' identity.

[269] See, for example, Yaya J. Fanusie, "Survey of Terrorist Groups and Their Means of Financing," Testimony before the House Financial Services Subcommittee on Terrorism and Illicit Finance, September 7, 2018, https://docs.house.gov/meetings/BA/BA01/20180907/108661/HHRG-115-BA01-Wstate-FanusieY-20180907.pdf.

The decentralization inherent in cryptocurrency has the potential to impede government regulation and hinder law enforcement efforts by virtue of its anonymization features. In the future, this threat could grow based on two factors: 1) cryptocurrencies successfully implementing privacy features that government agencies cannot overcome, and 2) the total market value of cryptocurrencies increasing, such that multiple extremely large transactions will not immediately stand out as suspicious.

Despite all the hype surrounding cryptocurrencies, they remain relatively unimportant in the consumer sphere. This may prove to be the most important factor in whether VNSAs adopt cryptocurrencies more widely. Should consumer-side innovation slow down, or should the value of cryptocurrencies decline significantly, it is possible that VNSAs' limited adoption of this technology could turn into outright abandonment.

What Is Cryptocurrency, Bitcoin, and Blockchain Technology?

While there is no consensus definition of cryptocurrency, the law firm Latham & Watkins provides a good synopsis:

> At the most basic level cryptocurrency—or digital currency or virtual currency—is a medium of exchange that functions like money (in that it can be exchanged for goods and services) but, unlike traditional currency, is untethered to, and independent from, national borders, central banks, sovereigns, or fiats. In other words, it exists completely in the virtual world, traded on multiple global platforms. These currencies are designed to incorporate and exchange digital information through a process made possible by principles of cryptography, which makes transactions secure and verifiable.[270]

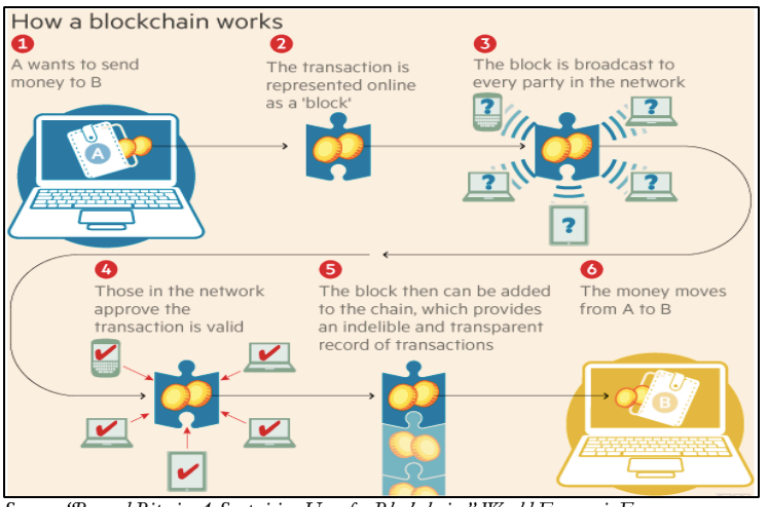
The technological cornerstone of Bitcoin and all other current cryptocurrencies is a public ledger known as a "blockchain." The blockchain is composed of digital blocks of data containing all pertinent information for every transaction. This information remains in chronological order, and is distributed to every computer "node" hosting the ledger. The blockchain records information about each transaction through the use of public and private "keys," made up of a string of numbers and letters unique to each account. The public keys are used to receive funds, while the private keys are used to send them. Together, they form the "wallet," which is a tool to access those Bitcoins.

This public process fosters trust that the digital currency cannot be "double spent," which occurs when the same currency is sent to multiple receivers from the same wallet. In the modern financial system, banks serve as a trusted third party that can ensure that an individual is not engaging in double-spending (for example, from a checking account), and thus promising to pay out money that she does not possess. But the blockchain does away with the need for a trusted third party: The ledger guards against double spending, allowing peer-to-peer exchanges of cryptocurrency without the need for banks to serve as an intermediary.

The ability to maintain a veil of privacy over cryptocurrency transactions comes from the use of private and public keys, which 1) are unique to each user, 2) hide identities through the use of an alphanumeric string,[271] and 3) specify the address or account of each user. An algorithm known as a

[270] Latham & Watkins, "Cryptocurrency: A Primer," 2015, https://www.lw.com/thoughtLeadership/LW-cryptocurrency-a-primer.
[271] One example of such a string is 5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreAnchuDf.

"hashing function" combines, or "hashes," the data and keys of both parties involved in every transaction. While this hashing function does not record the *identities* of the individuals involved in transactions, and thus allows for the anonymization for which cryptocurrencies are well known, the blockchain is a publicly available ledger containing every transaction that has occurred since the cryptocurrency's creation. This means that every transaction is viewable by anyone, but that individuals' identities are masked by the keys. Law enforcement thus has the ability to track individuals when they engage in a transaction with a website, market, or individual whose public key is known by authorities (*e.g.*, an online marketplace that has posted its public "key" online to receive Bitcoin as payment for goods). Thus, while cryptocurrency provides significant anonymity, the public nature of a blockchain prevents complete anonymity. Cryptocurrency transactions are therefore best considered pseudonymous rather than anonymous.



Source: "Beyond Bitcoin: 4 Surprising Uses for Blockchain," World Economic Forum.

For average users of Bitcoin, which remains the most popular cryptocurrency, buying Bitcoins is as easy as downloading an app, logging onto a Bitcoin exchange website, and creating a "wallet." The process is becoming even simpler with the development of Bitcoin ATMs and "point of service machines," which allow businesses to receive Bitcoin payment in person instead of strictly over the Internet. Bitcoin has served as a model and starting point for newer cryptocurrencies.

As of May 2019, there were 2,169 active cryptocurrencies. Altogether, these currencies were worth nearly $220 billion USD, but the distribution of market capitalization is extremely top-heavy. Fourteen of these currencies—including Bitcoin, Ethereum, XRP, and Litecoin—make up around 90% of the market cap.[272] But the explosion in popularity and diversity of cryptocurrency provides an increasing number of options to maintain privacy and anonymity when engaging in illicit financial transactions, despite the public nature of the blockchain ledger system.

One cryptocurrency, Monero, illustrates the upgraded privacy of some newer cryptocurrencies. While Monero may not be "fully anonymous and virtually untraceable," as was once suggested in a 2017 *Wired* article,[273] its enhanced security still increases its utility to VNSAs. It achieves this privacy in three ways: users can post "stealth addresses" that are not traceable to their original addresses; users can select to hide the amount being exchanged; and the underlying software allows for each exchange to include decoy coins from other users, such that an outside observer cannot determine who is sending the money, nor can they track when or where the actual money is spent.[274]

---

[272] "Cryptocurrency Market Capitalization," Coinmarketcap.com, https://coinmarketcap.com (accessed May 13, 2019).
[273] Andy Greenberg, "Monero, the Drug Dealer's Cryptocurrency of Choice, is on Fire," *Wired*, January 25, 2017, https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/.
[274] Aaron Van Wirdum, "Battle of the Privacycoins: Why Monero is Hard to Beat (And Hard to Scale)," *Bitcoin Magazine*, September 14, 2018, https://bitcoinmagazine.com/articles/battle-privacycoins-why-monero-hard-beat-and-hard-scale/.

Ethereum, another cryptocurrency descendant of Bitcoin, allows for the use of "smart contracts," which are digital contracts coded to complete the terms of the agreement without the need for in-person or third-party verification (*e.g.*, through a lawyer).[275] Cryptocurrencies like Monero that provide greater anonymity will be discussed in more depth later in this section.

Current VNSA Use of Cryptocurrency and Blockchain

At present, cryptocurrencies are rarely used by VNSAs for five key reasons:

1) Cryptocurrencies lack true anonymity. The public ledger attached to cryptocurrencies creates a vulnerability for users, as the ledger permanently records illicit transactions.

2) Because of the public nature of the ledger and the relatively low overall adoption of cryptocurrencies, it is difficult to transfer large sums of money without arousing suspicion.

3) Cryptocurrencies have not been widely adopted in many of the geographic areas where major VNSAs operate, thus limiting the utility of cryptocurrencies to satisfy these actors' most immediate needs. As Manheim et al. note in *Foreign Affairs*, "there is limited acceptance of digital cash in regions such as the Middle East and North Africa, where many terrorist groups are most active."[276]

4) The lack of a central reserve may necessitate multiple transactions when procuring large sums of cryptocurrency.

5) Group cryptocurrency holders must provide sufficient access to the wallet internally such that individuals within the group can readily utilize their funds. However, too much access creates an opportunity for personnel in the organization, or hackers, to steal funds.

Understanding these factors is important to anticipating future VNSA uses of cryptocurrency. If and when these barriers decline, the potential for VNSAs to incorporate cryptocurrencies more into their strategies will concomitantly rise.

Evidence of Usage by VNSAs and Criminal Networks

Use of cryptocurrency by criminal networks is a relatively recent phenomenon. In 2007, the U.S. Secret Service shut down an early cryptocurrency, e-Gold Ltd., due to its use in "extensive criminal activity," including money laundering.[277] In a more recent example from early 2017, a group of hackers stole data and intellectual property from HBO, and attempted to obtain ransom in Bitcoin.[278] By obscuring users' identities, cryptocurrency arguably lends itself to such operations.

---

[275] Dong He et al., *Virtual Currencies and Beyond: Initial Considerations* (International Monetary Fund, 2016), p. 23, https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf.

[276] David Manheim et al., "Are Terrorists Using Cryptocurrencies?" *Foreign Affairs*, April 21, 2017, https://www.foreignaffairs.com/articles/2017-04-21/are-terrorists-using-cryptocurrencies.

[277] Edward Lowery III, prepared testimony before the United States Senate Committee on Homeland Security and Governmental Affairs, November 18, 2013, https://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies.

[278] "Hackers Demand Millions in Bitcoin for Stolen HBO Files," *The New York Times,* August 7, 2017, https://www.nytimes.com/2017/08/07/business/hackers-demand-ransom-for-stolen-hbo-files.html.

There is strong evidence that terrorist organizations have used cryptocurrency for financing and weapons procurement, though it has still been limited in scope. The first known use of cryptocurrency by a terrorist organization originated in the Gaza Strip, when the Mujahedin Shura Council's media wing—the Ibn Taymiyya Media Center—called for Bitcoin donations to raise money for its fighters. This operation only raised 0.929 Bitcoins, worth $540 USD at the time.[279] Other groups have pursued similar strategies, typically with similar results. Al-Sadaqah, a group seeking to support Syrian insurgents, requested cryptocurrency donations; media groups Isdarat and Akhbar al-Muslimeen solicited cryptocurrencies; and Malhama Tactical, a private military contractor that works with Syrian insurgents, put out a call for cryptocurrencies to fund its services.[280] With respect to attack funding, Indonesian authorities have said that Daesh-linked individuals have used Bitcoin to fund terrorist activities in their country.[281] It also appears that Daesh used cryptocurrency, sent through Canadian cryptocurrency exchange CoinPayments, to fund at least part of the 2019 Easter bombings in Sri Lanka.[282] VNSAs have also been discussing cryptocurrency as an alternative means of covert funding and procurement for years.[283]

Potential VNSA Applications of Cryptocurrency

Should VNSAs choose to increase their use of cryptocurrencies, we present four ways in which they might do so.

Verified Personnel Payment. One area where cryptocurrency could potentially benefit VNSAs is verified personnel payment. The ease and security of cryptocurrency transactions could positively affect recruitment, as recruiters could provide "signing bonuses" or other economic incentives that previously may have raised a red flag for law enforcement.

Cryptocurrency could also be part of a "terrorist starter kit" that a militant organization provides to remote operatives to help them prepare for attacks. Such a starter kit could someday include access to a cryptocurrency wallet, in addition to tactical and strategic instruction. The ability to add a largely anonymous source of funding to the starter kit would improve remote operatives' chance of success. This "starter kit" principle could be adapted to serve the purposes of several kinds of VNSAs, including cartels and organized crime. Drug traffickers in need of local delivery personnel could send instructions and payment via the web, alleviating service delays or loss of market share.

Insurgent groups could also potentially use cryptocurrency to pay recruited foot soldiers and their families. Many fighters or supporters join insurgent VNSAs due to economic incentives. Ensured payments could provide an extra layer of reassurance and incentive to potential recruits. At present,

---

[279] Yaya Fanusie, "The New Frontier in Terror Fundraising; Bitcoin," *The Cipher Brief*, August 24, 2016, https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin.

[280] Yaya J. Fanusie, "Survey of Terrorist Groups and Their Means of Financing," testimony before the House Financial Services Subcommittee on Terrorism and Illicit Finance, September 7, 2018, https://docs.house.gov/meetings/BA/BA01/20180907/108661/HHRG-115-BA01-Wstate-FanusieY-20180907.pdf.

[281] Prashanth Parameswaran, "Indonesia Steps Up War Against Terrorism Financing," *The Diplomat* (Japan), April 12, 2017, http://thediplomat.com/2017/04/indonesia-steps-up-war-against-terrorism-financing/.

[282] Yashu Gola, "ISIS Used Bitcoin to Fund Horrific Sri Lanka Easter Bombings, Research Claims," *CCN* (Norway), May 2, 2019, https://www.ccn.com/isis-bitcoin-fund-sri-lanka-easter-bombings.

[283] See discussion in Aaron Brantly, "Financing Terror Bit by Bit," *CTC Sentinel* 7:10 (October 2014), p. 4, https://ctc.usma.edu/financing-terror-bit-by-bit/.

cryptocurrency is not widely accepted in key insurgent zones, thus limiting its use in this capacity. But insurgent groups may increasingly take advantage of paying recruits via cryptocurrency if they become more widely adopted while preserving anonymization features.

Procurement through Online Black Markets. Some early cryptocurrency users were drawn to the dark web, a corner of the Internet that requires special access through software like Tor. Though sites on the dark web function similarly to the regular Internet (aka the "clear web"), all traffic on the dark web is encrypted: thus the need to use Tor or similar services.[284] As Brill and Keen note, Tor is "a special network of computers on the Internet, distributed around the world, designed to conceal true IP addresses and therefore the identities of the networks' users. The Tor network is designed to make it practically impossible to physically locate the computers hosting or accessing the websites on the network."[285] In particular, criminals have coupled the anonymity of cryptocurrency with the access to illegal goods and services that can be found on the dark web.

Online marketplaces on the dark web sell illicit materials like drugs, guns, ammunition, fake passports, child pornography and stolen personal information. Silk Road, a pioneering platform for illicit activities, used Bitcoin as its sole medium of exchange before it was shut down by a U.S. government prosecution in 2013. Another black market, AlphaBay, was taken down by law enforcement in 2017. Indicative of the growing demand for online black markets, AlphaBay was significantly larger than Silk Road. The *New York Times* notes that it "grew into a business with 200,000 users and 40,000 vendors—or ten times the size of Silk Road."[286] Elsewhere on the dark web, one can find listings for assassins for hire, hackers for hire, weapons, deadly toxins, mercenaries who claim that they will torture your chosen victim, kidnappers, and similar services.[287]

VNSAs could use cryptocurrency to expand their capabilities through online black market purchases, as dark web marketplaces enable the outsourcing of criminal talent. But VNSAs also run the risk of getting scammed by these purported criminals for hire. Worse yet, an ad offering criminal services may actually be a law enforcement sting (though this risk can be mitigated by the VNSAs). Assuming the vendor is advertising legitimate services, cryptocurrencies can obscure the transactions, reducing paper trails. And the utility of cryptocurrencies for conducting such illicit activities without detection may be growing, given the development of more anonymous cryptocurrencies like Zcash, Dash and Monero.

In response to these and other concerns, authorities have ramped up efforts to identify and interdict dark web marketplaces. For example, in May 2019, German authorities took down the Wall Street Market, reportedly the second-largest marketplace on the dark web, and Finnish authorities shut

---

[284] Dan Patterson, "How the Dark Web Works," *ZDNet*, September 1, 2016, https://www.zdnet.com/article/how-the-dark-web-works/.
[285] Alan Brill and Lonnie Keen, "Cryptocurrencies: The Next Generation of Terrorist Funding?," *Defence Against Terrorism Review* 6:1 (Spring & Fall 2014), p. 20.
[286] Nathaniel Popper & Rebecca R. Ruiz, "2 Leading Online Black Markets Are Shut Down by Authorities," *The New York Times*, July 20, 2017, https://www.nytimes.com/2017/07/20/business/dealbook/alphabay-dark-web-opioids.html.
[287] See discussion in U.S. Department of Justice, press release, "Assistant Attorney General Leslie R. Caldwell Delivers Remarks at the ABA's National Institute on Bitcoin and Other Digital Currencies," June 26, 2015, https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-aba-s-national-institute.

down Valhalla, another prominent dark web market.[288] But according to Nicholas Christin, a dark web researcher at Carnegie Mellon University, the dark web is "resilient." It is likely that the void left by shuttered marketplaces will be filled.[289] VNSAs will likely remain able to procure illicit substances on the dark web in the future.

Cryptocurrency Theft and Hacking. Blockchain technology is practically invulnerable to external interference, manipulation, and theft. This is because all of the data on the blockchain is dispersed: There are hundreds, or thousands, of copies of the data that must be hijacked or corrupted in order to disrupt the blockchain.[290] But the personal computers and accounts of individual users and cryptocurrency exchanges are not. One of the most significant hacks directed at a major Bitcoin exchange occurred in 2014, when Japanese company Mt. Gox was hacked and lost around 850,000 Bitcoins, then valued at $460 million.[291] Other major cryptocurrency exchanges have been targeted as well.[292] Hackers have also targeted individual cryptocurrency users, trying to gain access to their online wallets. As of 2017, hackers had stolen an estimated $225 million from users of the cryptocurrency Ethereum, a sum totaling almost 1% of the entire market for that cryptocurrency.[293]

While there is no evidence that VNSAs have been behind the hacking of private cryptocurrency accounts, they could look to this as one method to raise funds illicitly. It is unlikely, however, that VNSAs will ever able to hack into mainstream cryptocurrencies themselves, rather than just stealing from individuals or exchanges. The blockchain itself is immune to hostile takeover unless a malevolent actor devoted a massive amount of hacking resources toward besting the system, a nearly impossible task, even for powerful state actors.

Money Laundering. Cryptocurrencies operate largely without formal regulation, creating an environment permissible for money laundering. Though cryptocurrency exchanges are often regulated, once fiat money is converted into cryptocurrency, it becomes more difficult to track. Trading money through various cryptocurrencies to obscure identities, transactions and locations may allow one to mask the true origins or destinations of illicit funds.

Fiat entry and exit points present the most challenging hurdles for VNSAs in the cryptocurrency money-laundering process.[294] But once the fiat currency is transformed into cryptocurrency, identity hashing in the blockchain and other privacy measures render it more discreet than traditional methods of disguising illicit funds. A criminal organization can use cryptocurrency "mixers" to further mask ownership of the funds. A mixer is a:

---

[288] Adi Robertson, "Police Just Took Down a Massive Dark Web Marketplace in Germany," *The Verge*, May 3, 2019, https://www.theverge.com/2019/5/3/18528211/wall-street-market-silkkitie-valhalla-dark-web-takedown-police-germany.

[289] Andy Greenberg, "Feds Dismantled the Dark Web Drug Trade—But It's Already Rebuilding," *Wired*, May 9, 2019, https://www.wired.com/story/dark-web-drug-takedowns-deepdotweb-rebound/ (quoting Christin).

[290] Robin Bloor, "Why is the Blockchain so Revolutionary?," *Medium*, May 14, 2018, https://medium.com/coinmonks/why-is-the-blockchain-so-revolutionary-explain-like-im-5-be3f6771f64c.

[291] Robert McMillan, "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster," *Wired*, March 13, 2014, https://www.wired.com/2014/03/bitcoin-exchange/.

[292] Jan Wieczner, "Hacking Coinbase: The Great Bitcoin Bank Robbery," *Fortune*, August 22, 2017, https://finance.yahoo.com/news/hacking-coinbase-great-bitcoin-bank-103035588.html.

[293] Ibid.

[294] Fiat entry and exit points refer to the point at which fiat money (government-backed currency) is exchanged for cryptocurrency (entry) or cryptocurrency is exchanged for fiat money (exit).

> Service where you could send your bitcoin, pay a small fee, and then receive different bitcoin than the ones that were sent. The successful bitcoin anonymization of these services depend[s] on the total number of users and coins available for mixing, which is why larger exchange sites and bitcoin shopping platforms were used more frequently. If an exchange was large enough, bitcoin could be deposited and withdrawn without being traded—effectively mixing the customer's original coins… [N]ot only do the peers not need to know about each other's destination address, but the mixing server helping to orchestrate the mixing doesn't know it, either.[295]

Further, tools like Dark Wallet render illicit money laundering even more anonymous. A report by Zachary Goldman at the Center for a New American Security notes that Dark Wallet seeks to prevent the de-anonymization of Bitcoin transactions. The report explains that the tool "disrupts the blockchain's potentially identifying aspects by combining random contemporaneous transactions and then encrypting recipients' information so it does not appear on the blockchain. This method explicitly seeks to enable illicit finance; as one of its founders stated, 'It's just money laundering software.'"[296] As we previously noted, other cryptocurrencies like Monero are harder to trace than Bitcoin.

Another possibility for VNSAs seeking to launder money through cryptocurrency is the use of front companies or straw purchasers at the point of entry. VNSAs' desired outcome is hard currency becoming cryptocurrency that is available worldwide, without being subject to the reporting requirements of a bank account. The first step would be to either find the right straw purchaser or else create a front company in a geographic area with few business regulations and little oversight. In order to mask the true purpose of the company, the VNSA could pose as a company accepting cryptocurrency as payment, thus providing a cover story to explain large sums of money being exchanged for cryptocurrency. For example, the creation of a gambling website might provide a plausible reason for possessing large sums of money and cryptocurrency. While there are no publicly reported instances of VNSAs using this system of money laundering, this is a potential scenario that would allow VNSAs to maximize the money-laundering advantage they might gain from the use of cryptocurrency.

[295] See https://www.coindesk.com/taxonomy-bitcoin-mixing-services-policymakers/.
[296] Zachary K. Goldman et al., *Terrorist Use of Virtual Currencies: Containing the Potential Threat* (Washington, DC: Center for a New American Security, 2017), p. 15.

Conclusion

VNSAs succeed and fail along many of the same axes as other organizations. For example, failing to incorporate new technologies can render VNSAs less effective than their VNSA competitors, and thus potentially render them obsolete. Unique to VNSAs, however, is that their success typically depends on evading authorities and state actors. This further increases the impetus to adopt new technologies. Indeed, VNSAs' survival may depend on their use of these new technologies.

It is thus vital to understand how VNSAs adopt new technologies. This study's primary contribution, the *VNSA technology adoption curve*, seeks to explain this process. As we have explained, this curve consists of four phases. The first phase, *early adoption*, is marked by a VNSA attempting to adopt a new technology, and disproportionately underperforming. The second phase is *iteration*, during which the consumer technology that the VNSA attempts to repurpose undergoes improvements driven by the companies that brought the technology to market. The VNSA similarly iterates with the technology. The third phase is *breakthrough*, where the VNSA's success rate significantly improves. The final phase is *competition*, where the VNSA's adversaries adapt to counteract its breakthrough.

A number of factors, including limited technological acumen, limited resources, and counter-measures, may delay—or even deny—VNSAs' successful adoption of new technologies. At the same time, certain VNSA-specific factors may enhance the likelihood that they successfully traverse the adoption curve. For example, the virtual plotter and drones examples suggest the importance of organizational structure, an abundance of resources, and a geographic safe haven as particularly important to VNSAs successfully adopting new technologies.

Daesh and other well-resourced groups—including cartels, Hizballah, and Aum Shinrikyo in its heyday—also had the resources to not only experiment with new technologies, but to incur repeated failures. Given that the *early adoption* and *iteration* phases of the adoption curve are characterized by limited success, a group's ability to reach the *breakthrough* phase may in part be a function of its resilience in the face of continued failure. Analysts assessing whether VNSAs will adopt certain technologies must consider organizational dynamics in addition to the availability and consumerization of the technologies.

It is our hope that by outlining VNSAs' process of technological adoption, this study will contribute to early recognition of danger signs, and to interdiction of VNSA attempts that pose the greatest risks to the public.