Extremism on the Horizon:

The Challenges of VEO Innovation and its Impact on Special Operations

Abstract

This paper identifies and discusses prospective patterns of emerging technology use in the 2020-2027 period by Violent Extremist Organizations (VEO) through the lens of the National Security Strategy and the Special Operations mission. The paper offers strategists and planners recommendations on how best to mitigate and address the emerging VEO technology use against U.S. national interests. Overall, this paper identified additive manufacturing, cryptocurrency, genome editing and synthetic DNA, robotics, commercial-off-the-shelf intelligence systems, and compounded technologies as the greatest potential challenges. This paper concluded that as the SOF enterprise postures itself to respond to the changes in VEO capabilities, it must prioritize relationships, maximize acquisition agility, and recruit differently. If SOF is to remain fit-for-purpose and continue to effectively advance the interests of the U.S. and its partners, it must change the way it does business today.

"Transnational threat groups, from jihadist terrorists to transnational criminal organizations, are actively trying to harm Americans. While these challenges differ in nature and magnitude, they are fundamentally contests between those who value human dignity and freedom and those who oppress individuals and enforce uniformity."

"To maintain our competitive advantage, the United States will prioritize emerging technologies critical to economic growth and security…"

- *U.S. National Security Strategy, 2017*

Introduction

September 11, 2001 was a stark demonstration that there are many groups in the world committed to creatively finding ways to harm the United States (U.S.). Since then, many more Violent Extremist Organizations (VEOs) with the will and capability to strike the homeland have emerged. Recently in Syria and Iraq, VEOs have demonstrated the ability to innovate rapidly across the physical, virtual, and cognitive realms. Their decentralized nature and lack of bureaucracy allow VEOs to innovate faster than the U.S. and other Western nations, and the relative limitations on VEOs' resources further incentivizes them to rapidly adopt technology that provides them asymmetric advantages. Simply put, without a dramatic change now, the U.S. stands to lose the technological advantage to VEOs that innovate proactively and rapidly as a matter of course.

This paper explores the anticipated technological advances VEOs may adopt from 2020-2027 the authors postulate will pose a persistent threat to the U.S. This time period was chosen in an effort to inform both planning and acquisition time horizons. Specifically, the authors will address the challenges and opportunities these technological advances will pose for Special Operations Forces (SOF) as they seek to protect and advance U.S. national interests abroad. Finally, this paper offers recommendations to the SOF Enterprise to mitigate the challenges that VEOs may present as they seek the innovation advantage on the battlefield of the future.

The data collection for this paper included unstructured and semi-structured interviews with subject matter experts and observational data from government entities, politicians, leading technologists, and technology companies [See Authors' Note]. Workshops and conferences were a valuable source of timely and relevant subject matter data relating to this paper's research. Secondary data came from credible institutions and recognized expert publications in the form of technical publications, blogs, academic articles, market research reports, and national security strategies. Using the data collected

and a variety of analytical methods, the below findings assess the prospective malicious use of emerging technologies by VEOs and offer recommendations for the SOF Enterprise.

Anticipated Technological Developments

Global innovation, the ability to share information quickly, rapidly advancing technology, and distributed knowledge have created new opportunities for politically hostile groups. Lower barriers to employ new technologies offer super-empowered individuals and VEOs a range of tools across the physical, virtual, and cognitive environments to pursue their malign objectives.[1] Arguably, technology is now advancing at such a velocity that a structured framework helps prioritize threats and resources. Diamandis and Kotler's "Six Ds" of exponential technology is one such framework to determine the impact and pace of growth for potential technologies, based on how far the technology has progressed. They argue that technology progresses along the following consecutive phases:

- **Digitized:** Once people digitize a physical commodity or service (represented in ones and zeros), it embarks on the first step of the exponential growth curve. This type of digital information is easy to access, share, and distribute.

- **Deceptive:** During the next phase of growth, the technology does not appear to expand quickly or make an impact. This period is often deceptively slow due to the nature of exponential change.

- **Disruptive:** The technology becomes disruptive once it outperforms other technologies in effectiveness and cost.

- **Demonetized:** In this phase, the technology becomes cheaper, and in some cases free, further reducing barriers for its use by actors with limited resources.

- **Dematerialized:** When advancements in technologies significantly reduce its size of the physical element of the technology and/or it is absorbed into other products (e.g., maps, radio, camera in mobile phone), it is considered dematerialized.

- **Democratized:** In the final stage of the exponential growth curve, the digitization, reduced cost, and dematerialization of the technology's original form result in the increasingly public access to the new technology.[2]

This paper uses the Six D's to evaluate the threats of six emerging technologies that VEOs could use: additive manufacturing, cryptocurrency, Genome Editing and Synthetic DNA, robotics and Commercial off the Shelf Intelligence Surveillance and Reconnaissance (COTS ISR). This list does not represent a comprehensive account of all technologies that

VEOs may leverage in the future. Instead, this list includes the top six technologies that either have reached the democratization stage or will reach it by 2027 and pose a threat to U.S. national interests, as visualized in Figure 1. The underlying element of these technologies is their use of digital information. It is the digital information that will activate the potential of these new technologies and may allow VEOs to employ force across the warfighting domains in new ways. Each of these six technologies is described in detail following Figure 1.

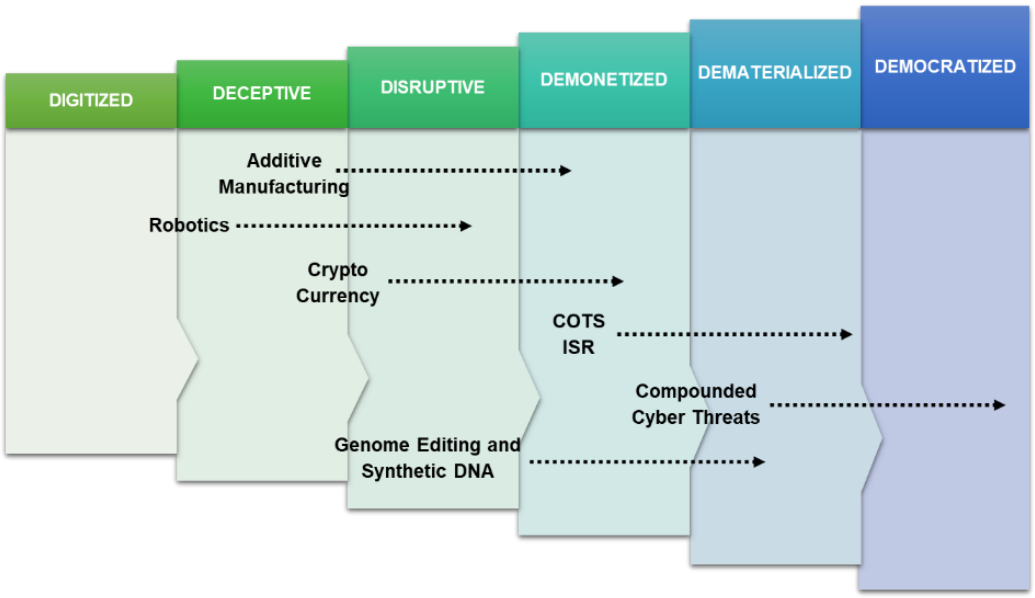

Figure 1 - Anticipated technological developments across the "D's" of technology growth interpreted for the malicious use of emerging technology posed by VEOs.

Additive Manufacturing

Although scientists developed additive manufacturing or three dimensional (3D) printing in the 1980s, 3D printing reached the democratization phase in the 2010s.[3] The internet allows the maker communities to create 3D designs through free software, share data and expertise through tutorial videos and create 3D objects. Today, countless companies offer 3D printing services with a click of a button. The democratization of this technology is of particular interest to VEOs as it affords them the potential to create unconventional weapons at scale.[4] SOF can anticipate that VEOs will leverage the accessibility of this technology to design and print unconventional fit-for-purpose weapons. Further, the next iteration of 3D printed weapons on the horizon is 3D printed explosives. While it is unlikely that this technology is yet in the hands of VEOs, they could gain this capability in the next seven years.[5]

Given these technological advancements, it is highly likely that VEOs will use additive manufacturing capabilities to 3D print weapons, design custom projectiles, and innovate with creative accessories. VEOs may seek to print 3D printed guns and share digital "weapon files" with likeminded individuals, bypassing arms control mechanisms and making attacks difficult to anticipate or prevent.

Cryptocurrency

A VEO's ability to recruit, self-organize, conduct attacks, and develop capabilities relies on funding. The secure blockchain platforms upon which cryptocurrencies operate have made illicit finance more difficult to track, stop, and prevent. At present, extremist organizations use cryptocurrencies to receive, manage, transfer, and spend money. Cryptocurrencies are transitioning from the deceptive phase of growth to the disruptive phase; as they gain traction in the mainstream, their use will also become more pervasive amongst VEOs. [6] Given the above, it is highly likely that VEOs will continue to leverage the anonymity of cryptocurrency to fundraise, launder money, and pay for goods and services while bypassing the regulated international financial system. This will allow VEOs the financial freedom of movement they require to operate in the shadows.

Genome Editing and Synthetic DNA

In the future, VEOs may continue to seek biological weapons and viruses as a means to attack the homeland.[7] Advancements in genome editing and synthetic DNA (e.g., synthetic viruses that can infect large populations, agroterrorism that can irreversibly destroy crops, and gene-drive editing which perpetually alters the evolution of the organism edited with unpredictable effects[8]) have increased the potential threat of these types of weapons. While specialists in the genomics field are demonetizing and dematerializing this technology through inexpensive kits and DNA editing software, such as Clustered Regularly Interspaced Short Palindromic Repeats (CRISPR), its use still requires a high level of expertise.[9] Considering these factors, it is very likely that VEOs will seek to acquire synthetic biology capabilities for malicious use. However, their ability to do so within the next seven years will be limited by the high technical skill needed to use the technology and weaponize it effectively. There is a low probability (but high risk) that a VEO could recruit an expert in this field who could overcome these challenges.

Robotics

VEOs are adept at employing Unmanned Aerial Vehicles (UAV), or "drones," on the battlefield. Initially, VEOs used Commercial-Off-The-Shelf (COTS) drones for reconnaissance and surveillance, later attaching explosive devices to deliver lethal effects. Currently, VEOs use them as a management tool to enable drone pilots to coordinate and assign vehicles to

locations to commit coordinated suicide attacks. The VEOs then leverage the video footage of these attacks for propaganda purposes.[10] Looking ahead, the character of conflict may change as VEOs develop ways to embed chemical, biological, radioactive, or nuclear (CBRN) substances into drone payloads. In the coming years, as VEOs gain access to Unmanned Underwater Vehicles (UUV), they could explore their use to strike vulnerable U.S. maritime targets.[11] Given these advances, it is highly likely that VEOs will continue to experiment with UAVs for surveillance and kinetic force application purposes in the operating environment. They may attempt to use swarms of drones to create confusion in the battlefield, allowing them windows of advantage to conduct follow-on attacks. It is very likely that if VEOs could obtain CBRN material, they would use drones as a delivery vehicle. This scenario is low probability but high risk. While initially VEOs may use UAVs for surveillance or trafficking goods, they could eventually progress to offensive attacks on friendly targets.

COTS ISR

Advances in artificial intelligence (AI) and the ubiquity of video surveillance have given rise to gait recognition technology.[12] Some systems "can identify people from up to 50 meters (165 feet) away, even with their back turned or face covered."[13] As the network of the Internet of Things (IoT) becomes more pervasive in public and private spaces, passive reconnaissance of movement will become more accessible. Researchers have developed a silent reconnaissance technology that uses radio frequency (RF) signals emitted by Wi-Fi devices to monitor individuals passively inside rooms and buildings.[14] This technology is publicly available and people may soon democratize it.[15] Considering the above, it is highly likely that VEOs may seek to leverage COTS ISR-related technology. An increasingly digitally connected world with sensors gathering sound, video, and signals will challenge SOF operators.

Compounded Cyber Threats: IoT, AI, and DeepFakes

In the future, one can expect that VEOs will seek to combine multiple cyber capabilities to further misleading or false narratives, targeting the U.S. and partner populations by creating content with DeepFake, IoT, and AI capabilities, and amplifying their messaging with social media. Friendly use of these capabilities has contributed to the development of smart infrastructure across industries (energy, agriculture, finance, health, transportation, etc.), the commercial reliance on digital infrastructure, and the digitization of homes with IoT. Together, these trends result in a growing number of digital and physical assets that VEOs can attack remotely. AI has already begun to change the character of these cyber threats.[16] As technology evolves, it will make these technologies more accessible. Arguably, VEOs may seek to use them to automate, accelerate, and further spread their cyber offensive actions.

With this in mind, it is highly likely that VEOs will seek to use DeepFakes, AI, and the IoT as a cognitive attack vector to sow doubt and confusion among their adversaries to advance their interests and narratives. If SOF lacks the capability to track and address these technologies, it may affect overall mission success. The next section provides strategic recommendations for the SOF enterprise to effectively address the challenges these technologies pose.

Strategic Opportunities and Recommendations

The SOF Enterprise has a record of unconventional thinking and creative use of force. This places SOF in an ideal position to tackle the employment of new technologies, or the repurposing of existing technologies, by VEOs. These developments come at a time where the Command is revising its strategy to reflect a new era of great power competition, actively seeking new technology through multiple means and channels, expanding partnerships, and investing in a Joint Military Information Support Operations (MISO) capability that cuts across combatant commands and aligns the SOF community. [17] Given the SOF mission and the current and anticipated use of new technologies by VEOs, this paper offers five overarching recommendations to best position the SOF Enterprise to respond from a position of strength.

Grow, Track, and Sustain Trusted Relationships

Effective rapid response requires accurate and timely intelligence; as the exponential growth of digital technology increases the pace of communications, this intelligence is ever more crucial. Cyber communications surveillance must be able to effectively anticipate VEO plans to 3D print weapons and monitor cryptocurrency transactions. As the VEO fight is global, international partners are key. At present, the SOF enterprise has a strong domestic and global network of trusted relationships. This network assists SOF operators during operations, serves as an early warning system for emerging hostilities, and crucially, helps SOF understand the environment and what courses of action would best deliver desired effects. One challenge, to this invaluable network is the core nature of military jobs, in which soldiers, sailors, airmen and Marines change roles every two to three years. This means that SOF must sustain relationships over decades despite frequent personnel changes. Ongoing relationships in the SOF network allow for a greater understanding of the problem sets and a memory of what worked in the past.

The SOF enterprise should create a database where it can track and map relationships so that incoming SOF operators can understand, leverage, and build the networks established by previous military personnel. Customer Relationship Management (CRM)-type software or social media-like platforms could be useful tools to map and build awareness of the human terrain in the operating environment. Concurrently, the global partnership

program should widen to encompass non-traditional partners, to include foreign and national technologists, sociologists, artists, makers, environment specialists, and patriotic hackers. Unconventional partners lead to increased unconventional thinking and insight, which could support asymmetric actions and unrestricted critical thinking, enabling the U.S. to proactively challenge VEOs.

Maximize Acquisition Agility

VEOs often test and adopt new technologies faster than nation-states, as they face fewer bureaucratic hurdles to procurement. When violent extremists change tactics with innovative use of technology (e.g., robotics, COTS ISR), they are not limited by procurement cycles that are fiscal year dependent. The nature of unconventional warfare in an era of rapidly developing technology requires the government technologies procurement system to be similarly cross-domain, easily modified, and agile. SOF should use platforms in a way that allows for rapid innovation that is not hampered by bureaucratic, slow, or inefficient processes. Increased acquisition agility will allow SOF to respond to new demand signals and changing VEO threats rapidly. Separately, the SOF enterprise should collaborate with U.S. Cyber Command (USCYBERCOM) to create joint periodic reports on related surveillance technology and capabilities that VEOs could use against SOF, so that operators can better posture themselves in their operating environments.

Close the Political-Military Divide

The SOF Enterprise is uniquely positioned to gather insights on VEOs and could advise U.S. political leadership about how to approach specific VEO challenges to U.S. national interests, including threats from emerging technologies. This paper recommends the creation of a channel for SOF operators to more effectively share insights with political leadership responsible for countering the VEO threat. This would close gaps of understanding about the reality on the ground and provide political leadership with insights from those who had first-hand experience and a sounding board for options to counter the threat. It would allow SOF to give political leadership a better perspective on the conflicts for which they create policy. This would also allow political leaders to learn more about the needs of SOF and their unique capabilities. One possible structure for this direct channel would be a meeting once or twice a year between SOF leadership and the Subcommittee on Intelligence and Counterterrorism in the House Committee on Homeland Security, and the Subcommittee on Crime and Terrorism in the Senate's Committee on the Judiciary.[18]

Recruit and Retain Talent with Cyber and Cognitive Expertise

VEO information and cognitive attacks could increase in scale, frequency and sophistication. SOF should build on their extensive experience and unique expertise in the area of cyber and psychological operations. This talent pool needs to master technologies that overlap virtual and cognitive areas, to include current and emerging forms of social media, the spatial web, cryptocurrency, and proficiency in the brain-machine interface. Finally, intergenerational perspective sharing on the social aspects of information technologies will be important, as new generations of SOF operators who are digital natives will have valuable insights on how to approach the new problem sets. SOF should tailor its recruitment activities to attract future operators with the relevant skill sets, create career opportunities for these individuals to ensure talent retention, and institutionalize a mechanism to encourage perspective sharing between current SOF operators and incoming experts.

Embrace Technological Advantage with Ethical Resolve

In an effort to act decisively in operating environments with moral confidence, SOF operators should undergo additional training on technology ethics in SOF contemporary and forward-leaning operational environments. For the SOF enterprise to best support operators and appreciate the emerging ethical questions and challenges they will face, the wider SOF Enterprise should also undergo this training. This will inform all personnel supporting SOF operators, from technologists to strategists, to acquisitions departments. Technologists and operational planners could have training on how to reflect doctrinal values and rules of engagement in the design of the AI algorithm. The training could be done at the Joint Special Operations University (JSOU) and the curriculum could pull from the certification "Ethics and Emerging Military Technology" program which has been running at the U.S. Naval War College since 2017.[19] The curriculum would then be adapted for the SOF enterprise and its mission. Acting with ethical resolve means that the SOF operators and all those who support them are aware of the new ethical challenges that the new technologies will bring.

Conclusion

The digital revolution, fusion of technologies, and innovation across elements of society such as smart cities, smart farming, advances in remote medicine, connecting machines through the IoT, and others are changing the world in unexpected ways. In the next seven years, the advancement and democratization of new technologies offer new possibilities for U.S. interests, while their potential employment by VEOs creates new challenges. The strategic recommendations described in this document offer SOF ideas about how to best position itself to address emerging challenges posed by exponentially changing technology to innovate, change, and grow.

Through 2027, it is highly likely that VEOs will remain a resilient and motivated adversary, one unhampered by bureaucracy that continually uses innovative means to use terror as a weapon for widespread effect. As SOF postures itself to respond to the changes in VEO capabilities, USSOCOM must prioritize relationships, maximize acquisition agility, and recruit differently. Simply put, if SOF is to remain fit-for-purpose and continue to effectively advance the interests of the U.S. and its partners, it must change the way it does business today.

DOD Disclaimer

In accordance with 5 CFR 2635.807, the disclaimer certifies the views presented are those of the speaker or author and do not necessarily represent the views of DoD, U.S. Special Operations Command, or its components.

Authors' Notes

To reduce limitations in the analysis of the research, the authors employed several research methods. Content analysis was used in this research to examine patterns of interest and priority themes in political statements and national security strategy documents including strategic guidance in efforts to understand key interests and identify patterns of interests and priorities. The interview data was analyzed for key interest areas and the oral presentations at conferences and workshops were analyzed to understand patterns of technological advancement that are taking place and will remain relevant in the 2020-2027 time frame. Sentiment analysis was used to gain insight into adversarial perspectives on its interests and how it sees the US. The data analyzed with this method was speeches and videos produced by adversaries.

Case study analysis was identified as a suitable form of empirical inquiry that investigates a phenomenon within its real-life context such as the scope of this research. Utilizing this descriptive and exploratory form of analysis, this research examines the malicious use of emerging technologies by VEOs. To a certain degree the Delphi Method is used in the subject matter interviews. Given that the SMEs have different backgrounds and are interviewed for different purposes not all questions will be the same and there are cases where follow up interviews are not necessary. This research is anticipatory and attempts to forecast actions and sequences of events through deductive reasoning based on: geopolitical realities, enduring national interests of the US and its adversaries, technological advances, research and investments, global economic shifts, environmental considerations.

References

[1] Adam Elkus, A. and Burke, C., (2010), WikiLeaks, Media, and Policy: A Question of Super-Empowerment, Retrieved from https://smallwarsjournal.com/blog/journal/docs-temp/558-elkus.pdf

[2] The 6 Ds of Exponential Growth, from the book Bold by Peter Diamandis and Steven Kotler https://singularityhub.com/2017/12/29/what-are-the-6-ds-of-exponential-organizations/

[3] 3D Printing Industry (2019). History of 3D Printing. https://3dprintingindustry.com/3d-printing-basics-free-beginners-guide#02-history

[4]Dearden, L. (2019). Use of 3D printed guns in German synagogue shooting must act as warning to security services, experts say. Independent UK. https://www.independent.co.uk/news/world/europe/3d-gun-print-germany-synagogue-shooting-stephan-balliet-neo-nazi-a9152746.html

[5] Los Alamos National Laboratory (2016). Explosiv3Design. https://www.lanl.gov/discover/publications/1663/2016-march/explosive-3d-design.php

[6]Schoeberl, Richard. (2018). Gene Drives – An Emerging Terrorist Threat. Domestic Preparedness. https://www.domesticpreparedness.com/preparedness/gene-drives-an-emerging-terrorist-threat/

[7] Memri (2018). Pro-ISIS Media Outlet Circulates Video Calling for Biological Attacks in the West. Middle East Media Research Institute TV Monitor Project. https://www.memri.org/tv/pro-isis-video-calls-for-biological-attacks-in-the-west/transcript

[8]Schoeberl, Richard. (2018). Gene Drives – An Emerging Terrorist Threat. Domestic Preparedness. https://www.domesticpreparedness.com/preparedness/gene-drives-an-emerging-terrorist-threat/

[9] Sneed, Annie. (2017). Mail-Order CRISPR Kits Allow Absolutely Anyone to Hack DNA. Scientific American. https://www.scientificamerican.com/article/mail-order-crispr-kits-allow-absolutely-anyone-to-hack-dna/

[10] Balkan, Serkan. (2017). DAESH's Drone Strategy: Technology and the Rise of Innovative Terrorism. SETA. https://www.setav.org/en/daeshs-drone-strategy-technology-and-the-rise-of-innovative-terrorism/

[11]Suguna, VS. Rahman, Faizal. (2018). Aquatic drone terror attacks a growing possibility. Today Online. https://www.todayonline.com/commentary/aquatic-drone-terror-attacks-growing-possibility

[12] Giles, Jim. (2012). Cameras know you by your walk. New Scientist. https://www.newscientist.com/article/mg21528835-600-cameras-know-you-by-your-walk/

[13] Kang, Dake. (2018). Chinese 'gait recognition' tech IDs people by how they walk. AP News. https://www.apnews.com/bf75dd1c26c947b7826d270a16e2658a

[14] Yanzi Zhu, Zhujun Xiao, Yuxin Chen, Zhijing Li, Max Liu, Ben Y. Zhao, Haitao Zheng. (2019). Et Tu Alexa? When Commodity WiFi Devices Turn into Adversarial Motion Sensors https://arxiv.org/pdf/1810.10109.pdf

[15] Vincent, James. (2019). New AI deepfake app creates nude images of women in seconds. The Verge. https://www.theverge.com/2019/6/27/18760896/deepfake-nude-ai-app-women-deepnude-non-consensual-pornography

[16] Warner, Bernhard. (2019). Artificial Intelligence Is About to Make Ransomware Hack Attacks Even Scarier. Fortune. https://fortune.com/2019/06/21/ai-ransomeware-hack-attacks/

[17] Military Times. (2019). Less door kicking, more partner building for special operations in 'great power competition'. https://www.militarytimes.com/news/your-military/2019/04/10/less-door-kicking-more-partner-building-for-special-operations-in-great-power-competition/

[18] Subcommittee on Crime and Terrorism in the Senate's Committee on the Judiciary https://www.judiciary.senate.gov/about/subcommittees/subcommittee-on-crime-and-terrorism

[19] Public Affairs Office USNWC. (2019). Ten U.S. Naval War College Students Earn Ethics and Emerging Military Technology Program Certificates. https://usnwc.edu/News-and-Events/News/Ten-US-Naval-War-College-Students-Earn-Ethics-and-Emerging-Military-Technology-Program-Certificates