On the Horizon: Security Challenges at the Nexus of State and Non-State Actors and Emerging/Disruptive Technologies

A Strategic Multilayer Assessment (SMA) Periodic Publication

April 2019

Contributing Authors: Gary Ackerman (University at Albany), R. E. Burnett (National Defense University), Bennett Clifford (George Washington University), Rebecca Earnhardt (University at Maryland), Thomas Holt (Michigan State University), Gina Ligon (University of Nebraska Omaha), Michael Logan (University of Nebraska Omaha), Robert McCreight (George Mason University), Don Rassler (Combating Terrorism Center at West Point)

Opening Remarks provided by: Brig Gen Alexus Grynkewich (JS J39), Matthew Clark (DHS), & Glenn Fogg (DASD(EC&P))

Editor: Georgia Harrigan (Department of Homeland Security Science and Technology Directorate)

Integration Editor: Mariah C. Yager (JS/J39/SMA/NSI)

SMA White Papers and reports can be downloaded from http://nsiteam.com/sma-publications/

Disclaimers

The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

Mention of any commercial product in this paper does not imply Department of Defense (DoD) endorsement or recommendation for or against the use of any such product. No infringement on the rights of the holders of the registered trademarks is intended.

The appearance of external hyperlinks does not constitute endorsement by the United States DoD of the linked websites, or the information, products or services contained therein. The DoD does not exercise any editorial, security, or other control over the information you may find at these locations.

OPENING REMARKS: Joint Staff J39 PERSPECTIVE

Brig Gen Alexus Grynkewich, Joint Staff J39, Deputy Director of Global Operations

As we look forward toward what is still an emerging and thus indefinite security environment, we should be mindful that the technological advances we see today will inevitably change how we define threats to US national security; how we think about defense strategies, operational activities, and planning; and how we conduct missions at the tactical level and operational levels.

To date, the defense and research and development (R&D) communities have focused on advances in areas such as rapidly expanding access to and operations in space; access to nearly global communications technologies; and on technological advances with more obvious military implications, such as electronic warfare and missile technology. However, if we broaden our focus as suggested by the contributors to this white paper, we also see enormous military implications in emerging areas of science and technology, including genomics and digital biology, advanced materials, automated knowledge work, and energy storage. Others surely lie in areas well past what we can imagine today.

While the full nature of the future security environment is still uncertain, one thing is clear. The same exciting technologies that promise to enhance human understanding and decision-making will also impact our ability to defend the homeland and respond to collective threats to allies and partner nations. There will be enormous opportunities, and potentially enormous future threats.

The obvious implication is that we must be as committed to adapting our organizational cultures, mindsets, and defense concepts as we are to adapting technologies. It should become routine to consider the human dimensions of technological change. Even on a social level, the behaviors and decisions involved in communicating with others have changed in ways inconceivable before the advent of smart phones. As is so well illustrated by the pieces contained in this volume, in order to avoid asymmetric and strategic surprise, operators *at all levels* must have the training and education needed to understand the criticality of social and political contexts of human conflict. While mastery of technology will still be necessary, it will no longer be sufficient.

Just as new technologies are the result of creative and uninhibited conceptualization by technologists and engineers, we must allow innovation and creativity of thought—what we might call 'disruptive thinking'—along with assessment of disruptive technologies. This is, at its essence, a bureaucratic problem. We need critical thinking to recognize and exploit emerging and future technologies that will allow us to retain an advantage over competitors. We need to be able to distinguish technological advances that safeguard from those that disrupt. The articles in this white paper provide government stakeholders—intelligence, law enforcement, military, and policy agencies—with valuable insights and analytic frames to help get us there.

OPENING REMARKS: DHS Perspective

Matthew Clark, Department of Homeland Security Science and Technology Directorate

The production or distribution of dangerous technologies by adaptable adversaries, whether nation states or non-state actors, will continue to grow. No government entity will be able to halt the resulting attacks and their consequences completely. Defensive preparation and mitigation are our principal options. Even then, we need to be selective and efficient in mounting our defenses. For example, eliminating access to new software and information technologies is difficult, perhaps futile, given the capacity for near-instantaneous distribution to anywhere in the world. Similarly, engineered bio-threats will continue to multiply, and new forms will be weaponized and distributed widely in a short period of time.

Given the sophistication of techniques like gene manipulation and the ubiquity of cyber weapons, to name two threats, the US ultimately will face some consequences of these threats. The extent of those consequences is what we need to tackle. Some of the greatest damage has been done by trusted actors who delivered substances, plans and intelligence to adversaries. The threat was not sophisticated technologies or biological agents, but defects in the human psyche that caused some to betray their compatriots in support of inhumane causes and practices.

The Department of Homeland Security shares the responsibility of countering consequential threats including cyber, biological, chemical, and radiological. In which of these area should we invest in defense or mitigation, and how do we prioritize our investments? A comprehensive analysis that compares simultaneous defense against multiple threats versus sequentially building our defenses in priority order based on the severity of consequences is not available. This suggests that an analysis of how to sequence deterrence investments would be a fruitful area for future research.

OPENING REMARKS: OSD Perspective

Glenn Fogg, Office of the Deputy Assistant Secretary of Defense for Emerging Capability & Prototyping

As we face an era of what seems to be a state of unending asymmetric conflict, the US has to prioritize its attention on Great Power Competition while also continuing to focus on the risks from other types of relevant malevolent actors that could harm US and global interests. The last few decades saw the rise of unprecedented violent extremist organizations, which became the major US foreign policy focus. As a result, near-peer adversaries took advantage of the US's diverted attention and gained in strength and capability. We cannot allow ourselves to ignore this organic space that may permit the evolution of events to adapt and grow unchecked. Instead, we need to reframe our thinking about non-state actors and their environments, and focus on what type of power is relevant in the emerging strategic global environment.

This White Paper in small ways tries to conceptualize the evolving danger of non-state actors and evolving technologies at a time when both Great Power Competition and asymmetrical activity are a simultaneous threat to world order. Innovation and new technologies have many positive attributes and provide significant improvement to humanity. Many of these improvements were likely unforeseen at the time of initial discovery. However, the unpredictability of the technology trajectories can lead to significant negative consequences. The overall future trajectory of modern technologies hinges on a fairly imperfect and periodically naïve grasp of dual-use science and technology and what it portends for our planet and its inhabitants. As pointed out by one of the authors "…One immediate concern is to determine not only how it (technology) is affecting our current way of life, geopolitics, the economy, social stability, governance, security, and the ordinary functions and determinants of the natural world around us, but also weigh the downstream consequences of technology growth, diversity, and convergence on all of those things ten to twenty years on…"

This white paper aims to discuss certain leaps in innovation and understand what this means for national security. Some example items discussed in the white paper

- Terrorism provides a model context for examining creativity, as the need for survival and innovation pervades these destructive and malevolent groups.
- The rise of online illicit markets that enable the sale of cybercrime tools and stolen personal information have made it possible for individuals to engage in technically sophisticated forms of crime regardless of level of computer skill
- As terrorists engage in increasingly lethal and technologically sophisticated attacks, the concern surrounding terrorists acquiring cutting-edge weaponry and related technologies is accumulating
- The increasing convergence between the fields of biosecurity and cybersecurity may result in consequences that analysts have yet considered
- The Islamic State's drone accomplishments speak to the character and style of future threats that are either constructed around or that significantly leverage dual-use commercial technologies — and how other, similar types of dual-use technology derived threats might be better mapped and detected

- Conflict where autonomous weapons are employed that utilize AI lethal decision-making and simultaneously employ social media tools and other digital tools to alter, confound, and manipulate facts toward an engineered version of events.

Bottom line: Emerging science and technology will continue to disrupt customary characteristics of political and kinetic conflicts among states and non-state actors.

Executive Summary

Innovation and new technologies have many positive attributes and provide significant improvement to humanity, much that is likely unforeseen at the time of initial discovery. The unpredictability of the technology trajectories can lead to significant negative consequences. This white paper aims to discuss the massive leaps in innovation and understand what this means for national security.

The articles are briefly summarized below.

In **Chapter 1**, entitled "Third Offset Implications for Homeland Security: Tranquility or Turbulence," **Robert McCreight** states that the overall future trajectory of modern technologies hinges on a fairly imperfect and periodically naïve grasp of dual-use science and technology and what it portends for our planet and its inhabitants. He goes on to say that one immediate concern is to determine not only how it is affecting our current way of life, geopolitics, the economy, social stability, governance, security, and the ordinary functions and determinants of the natural world around us, but also weigh the downstream consequences of technology growth, diversity, and convergence on all of those things ten to twenty years on. If advanced dual-use technologies hold the potential for a vast array of unanticipated threats in the next few years, we will need effective doctrine, strategy, and deterrence measures. He asks a key question: How to begin to establish criteria which guarantees that humans retain ultimate control, management, and direction of advanced dual-use technologies and thereby thwart untoward and dangerous outcomes arising from their mix of expected and unexpected outcomes. He advances five possible criteria for wrestling with the emergence of ADUCT (advanced dual-use convergent technologies) in a manner that sketches out an approach for the short term and allows flexibility for modifications and improvements along the way over the next decade.

Gina Ligon and **Michael Logan** in **Chapter 2**, "Malevolent Innovation: Novelty and Effectiveness in Terror Attacks," state that terrorism provides a model context for examining creativity, as the need for survival and innovation pervades these destructive and malevolent groups. Despite this, creativity and innovation remain underdeveloped concepts in terrorism research. One reason for this is the limited empirical data about this phenomenon, making it unclear which tenets of creativity research hold versus which do not translate in the domain of terrorism. The present effort overcomes this by examining the dimensions of malevolent innovation in a large sample of terrorist attacks. To anticipate adversary threats, it is critical that we examine all of the possible combinations of VEO innovation developed in the past. This particular effort can provide planners with exemplars of the highest levels of VEO innovation across a large dataset of violent extremist organizations, providing a comprehensive look at what is possible and what should be prevented.

Don Rassler in **Chapter 3** "Back to the Future: The Islamic State, Drones, and Future Threats" states that the Islamic State is an irony of sorts, as while the organization looks to, is inspired by, and seeks to recreate the past certain aspects of the group's behavior also provide a window into conflicts of the future. A key case study in this regard is the Islamic State's drone program, and specifically how the group "overcame technical and cost asymmetries," and creatively developed a novel and scalable drone-based weapons system "constructed from commercial components that challenged—at least for a period of time—states' ability to respond." He goes on to state that the Islamic State's drone accomplishments speak to, and have a number of important implications regarding, the character and style of future threats that are either constructed around or that significantly leverage dual-use commercial technologies. He concludes by stating to stay ahead of the issue, and to better prepare for a future that will almost certainly be typified by the proliferation of other hybrid threats that leverage and/or repurpose commercial systems in dangerous ways, the United States should identify

the pathways and methods that allowed the Islamic State to acquire and scale its fleet of quadcopter drones in the first place, and trace the evolution of functional threat streams.

Bennett Clifford in **Chapter 4,** "Exploring Pro-Islamic State Instructional Material on Telegram," makes several key observations:

- English-speaking supporters of the Islamic State (ISIS) use the messaging application Telegram to distribute a range of information, including instructional material—manuals and guides designed to aid operatives with step-by-step procedures for providing assistance to the group.
- Channel administrators distribute whichever manuals they believe can be of aid to aspiring operatives, regardless of its ideological background.
- Telegram's internal file-sharing features and lax approach to content moderation allow channel administrators to create repositories of instructional information within Telegram channels.
- While attack-planning manuals available on Telegram channels understandably pose a large concern for counterterrorism authorities, operational security and cybersecurity manuals are also frequently distributed, relatively easy to implement, and help operatives successfully conduct activities in support of terrorist groups while minimizing the risk of detection or apprehension.

In **Chapter 5** entitled "Examining the Present and Future Role of Cybercrime-as-a-Service in Terror and Extremism," **Thomas Holt** makes the case that the rise of online illicit markets that enable the sale of cybercrime tools and stolen personal information have made it possible for individuals to engage in technically sophisticated forms of crime regardless of level of computer skill. Ideological and terror groups over the last decade have expressed an interest in cyberattacks as a means to cause harm, though it is not clear how much ability they have to perform such attacks. As a result, cybercrime markets may engender their attacks, though it is not clear how often this may occur, or what conditions would lead to their use. He provides recommendations for policy and research to disrupt cybercrime markets and improve our knowledge of ideologically-motivated cyberattackers generally.

- Cybercrime markets generate millions of dollars in revenue and enable non-technical actors to perform sophisticated attacks.
- They may provide a point of entry for ideologically-motivated extremists and terrorists to engage in cyberattacks.
- These markets can be disrupted through traditional law enforcement investigations, and may also be affected through other extra-legal efforts such as Sybil attacks.
- Research is needed on the radicalization process of ideologically-motivated actors who engage in cyberattacks, and how this differs from those who have engaged in physical attacks.

Rebecca Earnhardt and **Gary Ackerman** in **Chapter 6** entitled "Modelling Terrorist Technology Transfer," make the point that while technology transfer occurs as a part of routine life, the topic remains relatively understudied in the terrorism literature. As terrorists engage in increasingly lethal and technologically sophisticated attacks, the concern surrounding terrorists acquiring cutting-edge weaponry and related technologies is accumulating. They go on to describe the Terrorist Technology Transfer (T3) project which provides a first cut at addressing this critical operational gap in knowledge through the exploration of extant technology transfer literature, construction of the first

iteration of the T3 Model, and illustrative application of the model to an emerging technological threat. They conclude by stating the T3 project indicates the promise of having not only research, but also operational and policy impacts. It raises the possibility of providing government stakeholders, including intelligence, law enforcement, military, and policy agencies with a variety of insights and operational tools

In **Chapter 7,** "Hacking the Human Body: The Cyber-Bio Convergence," **Rebecca Earnhardt** makes the point that the increasing convergence between the fields of biosecurity and cybersecurity may result in consequences that analysts have yet considered. Biotechnology use and expertise expansion beyond practitioners have stoked concerns about a wide range of traditional biosecurity issues including shielding the outputs from advanced gene editing systems or protecting university lab data storage systems. As biotechnology advances, including digitization and automation of systems that were once localized and only accessible to those directly involved on related research, biosecurity and cybersecurity fields continue to intersect. She concludes by stating a fully-fledged research project would explore the cyber security risk factors that are cited commonly as key vulnerabilities, and filter these cyber security risk factors through an adversary technology adoption decision making and motivational analysis.

In **Chapter 8** entitled "Evolving Human and Machine Interdependence in Conflict: Advantages, Risks, and Conundrums," **R. E. Burnett** makes several key points:

- Emerging science and technology will continue to disrupt customary characteristics of political and kinetic conflicts among states and non-state actors.
- The increasing complex interdependence between humans and machines is one area for particular examination.
- We cannot reliably predict whether or not human roles will rapidly give way to a more dominant robotic style of war, so we must prepare for a variety of futures, per the Scharre/Horowitz autonomy typologies.
- Humans involved with machines that operate at vastly greater speeds and volumes of data will further create problems of cognitive demand for the human soldier that need to be examined.
- We must investigate this not only in terms of technical performance, but also from a more holistic perspective, to include the social, political, and psychological dimensions of the soldier and of the citizen.

Contents

Acronyms

ADUCT	advanced dual-use convergent technologies
AI	artificial intelligence
DICE	Division of Industry and Consumer Education
DIY	Do-It-Yourself
DHS	Department of Homeland Security
DoD	Department of Defense
GTD	Global Terrorism Database
ICD	implantable cardiac device
IED	improvised explosive device
IMD	implantable medical device
ISIS	Islamic State
ISR	intelligence, surveillance, and reconnaissance
LEADIR	Leadership of the Extreme and Dangerous for Innovative Results
MTI	malevolent tactical innovation
R&D	research and development
SME	subject matter expert
ToS	Terms of Service
T3	Terrorist Technology Transfer
UAS	unmanned aerial systems
UAV	unmanned aerial vehicle
VEO	violent extremist organization
VNSA	violent non-state actors

Chapter 1. Third Offset Implications for Homeland Security: Tranquility or Turbulence?

Robert McCreight
George Mason University
remc48@gmail.com

Background and Theory

The overall future trajectory of modern technologies, especially the fully complex spectrum of unexpected as well as expected positive and negative outcomes, hinges on a fairly imperfect and periodically naïve grasp of dual-use science and technology and what it portends for our planet and its inhabitants. One immediate concern is to determine not only how it is affecting our current way of life, geopolitics, the economy, social stability, governance, security, and the ordinary functions and determinants of the natural world around us, but also weigh the downstream consequences of technology growth, diversity, and convergence on all of those things ten to twenty years on. It is a vastly ambiguous scenario which includes risks of both tranquility and turbulence. If advanced dual-use technologies hold the potential for a vast array of unanticipated threats in the next few years, we will need effective doctrine, strategy, and deterrence measures. That means we should be weighing the implications of all of this and deciding what should be done about it?

The Quest for Criteria and the ADUCT Dilemma

We can easily envision the linear extrapolation of advanced technologies in genomics, nanoscience, and neuroscience paving the way for a more resilient, vigorous, and robust contributor to better human health. Better brain science allows us to curb Alzheimer's disease, dystrophy, and perhaps autism could result. Breakthroughs in nanogenomics could lead to targeted treatment of cancer and devastating maladies which have plagued humans for centuries. However, dual-use science and technology requires that we grasp that remote external manipulation of thought and perception is possible; that nanogenomics opens to door to unexpected nefarious bioweapons; and that mergers of AI, robotics, and laser technology may usher in an era of lethal autonomous cyborgs impervious to kinetic control and submission.

This scenario begs the question of how we begin to establish criteria which guarantees that humans retain ultimate control, management, and direction of advanced dual-use technologies and thereby thwart untoward and dangerous outcomes arising from their mix of expected and unexpected outcomes. Beyond a 'kill switch' approach, we find that in a global arena of advanced dual-use technologies where no treaties, or universal norms and injunctions stem the steady growth of malevolent convergent technology responsible nations need a firewall against emerging hyper-strategic weapons almost immediately.

In turn, nations committed to global security, regional peace, stability, and international cooperative commonwealth can ill afford to allow advanced dual-use convergent technologies (ADUCT) to run rampant and alter the strategic balance. If no natural safeguards, curbs, or restrictions exist to negate the worst and most damaging effects of the ADUCT then a genuine dilemma emerges—**How to govern, direct, control and manage the emergence and growth of ADUCT on a global scale while retaining each nation's sovereign options for self-defense against an uncontrolled ADUCT threat**?

This challenge calls for the immediate consideration of criteria to provide a framework for the control, management, and governance of ADUCT before its unrestricted continuation poses a threat to the peace, stability and security of nations. Consider the following five items.

Looking at Five Criteria for the Emergence of ADUCT

One avenue for assessing the impact of ADUCT for the 2020-2030 period considers the extent to which the apparent absence of global consensus on the ADUCT issue and its remedy indicates that the United States must either prepare itself now regardless of what other nations chose to do, or collectively encourage leading nations of the world to open frank discussions on the subject with an eye towards finding elements of an agreed strategy and interim solution. Of course, the US can do both or neither, but allowing ADUCT to evolve without some overarching contingent strategy seems dangerous at best.

Given the current choices, one outcome seems more attractive than the others. It is likely the US ought to prepare itself for a combination of strategic, economic, technological, and operational reasons to fashion its own approach and philosophy until or unless a wider global awareness of the imperative for a collective ADUCT plan of engagement appears.

That brings us closer to an examination of five possible criteria for wrestling with the emergence of ADUCT in a manner that sketches out an approach for the short term and allows flexibility for modifications and improvements along the way over the next decade. The US Government must wrestle with these questions now or risk facing elements of strategic surprise over the next 10 years.

First and foremost, the overall national effort should involve key technology agencies of the federal government in partnership with leading academic, private sector, and entrepreneurial interests in a mechanism brokered by the Office of Science and Technology Policy but accountable to the Vice President. Here the purpose is to define and sketch out national level ADUCT policy principles and direction.

A **second** dimension is the thoughtful generation of white papers, expert simulations, tabletop games and case studies which help organize the ADUCT set of issues into reasonable priorities. Exercises and tactical in depth discussions of the threats and opportunities which ADUCT symbolizes are key here.

Yet a **third** aspect of the approach entails involving state and local governments, civic institutions, and community leaders in a transparent technical discussion of the full spectrum of ADUCT issues and the need to reign in, or manage, and redirect exiting ADUCT enterprises—including an assessment of results and outcomes—that are deemed largely beneficial to the community. The net byproduct is a serious technology assessment of likely outcomes seen as NOT beneficial.

Looking at a **fourth criteria** related issue embedded in ADUCT is enlisting government, private sector, and academic experts to engage in a systematic assessment of immediate, mid-term, and long-term implications of various cutting edge technologies in terms of their societal, political, economic and security impact on the US and our global partners.

The **fifth and final criteria** for deducing what ADUCT means and implies for the global community of sovereign nations and its security implications for the US, is a candid risk assessment of the

weaponization pathways and options which might directly or inadvertently flow from unrestricted research into ADUCT. Here the focus is on nefarious clandestine efforts to proliferate via ADUCT or alter the strategic balance. This might be accomplished within NATO or similar alliances apart from any UN sponsored venture of its kind.

In turn, another set of credible criteria is urgently needed to guide discussion and deliberation on the full gamut of ADUCT matters merits under consideration with an eye towards suggesting mechanisms to better understand how to manage, control, and govern what the future seems to be delivering.

Briefly, these candidate criteria designed to guide decision makers include themes under which ADUCT is evaluated and measured in terms of its inherent value, risk, and importance to an enduring American society. These are:

- ***Governance and social stability*** which refers to the extent to which ADUCT improves, undermines, increases, or diminishes organs of government and social stability to continue their operation without major disruption or discontinuity;
- ***National Risk management*** which refers to the extent that ADUCT economic, societal, and strategic risks [positive or negative] can be weighed by experts before further advancements and refinements to the technology are permitted or encouraged;
- ***Military doctrine strategy and deterrence*** which refers to the development of military doctrine, strategy, and deterrence policies and procedures as they pertain to ADUCT;
- ***Benign benefits*** which refers to the product of experts assessing the full measure of expected benefits to society, the economy, and governance of continued ADUCT research;
- ***Disruptive effects*** which refers to the product of experts assessing the full spectrum of disruptive and destructive effects of ADUCT on governance, society, or our economy;
- ***Geopolitical influences*** which refers to leadership experts in government, business and society gauging the net positive and negative effects [including expected and unexpected outcomes] on geopolitical factors such as state stability, international security, global health, economic development, and regional security.

The overall approach to ADUCT and adoption of a decades long strategy assumes that for the United States, funded efforts would be launched in 2019 among key federal agencies [led by DHS and DoD] to focus and extend comprehensive consideration towards a detailed plan, process and method of analysis which enables action to be taken. Strategic aspects of ADUCT are deserving of utmost priority as the global environment tends to support continued evolution and growth of ADUCT among rival nations such as Russia, China, the EU, and several other Asian nations. Currently, there are no indications that any steps involving counter proliferation or trade controls are in place among nations at risk to regulate, direct, control, or collectively manage the steady growth of ADUCT within or amongst their borders. Accordingly, we should conclude that continued proliferation of ADUCT research and shared ventures among these nations, and outside sovereign intelligence scrutiny, is to be expected.

As a result, the net impact of ADUCT on homeland security is deeply complex and uncertain as it appears new technologies and potential weapons systems may emerge in the 2020-2030 period which could fundamentally alter the security landscape against which DHS and DoD must prepare a coherent strategy. There is no point in waiting until a newly emerging mixed, hybrid, or convergent technology appears that has profound security implications for homeland security and the overall national security of the United States. Being reactive and untimely negates the best chances for

securing any strategic leverage or deterrence against a nascent new threat, even if originally discounted as unlikely, which may exert a wholly disruptive ripple effect on regional stability.

Approaches, ideas, innovative strategies, and specific plans are needed to deal with the risks of ADUCT becoming a new and formidable threat over the next five to ten years. Key agencies of the US government must grapple today with the full spectrum of immediate and long term ADUCT risks even if they are imperfectly understood. Against a tidal shift in strategic technologies the lack of awareness, distraction or misplaced threat analysis can inflict serious unexpected consequences.

The urgency of dealing with ADUCT itself as a mega-strategic issue cannot be underestimated. Key federal agencies including DHS, together with DoD, must consider the risks of emergent ADUCT threats as we enter the third decade of the 21st century. They must define, characterize, and prioritize the shape of ADUCT as a broad and revolutionary phenomenon equivalent in scope and impact to the discovery of electricity and the atom bomb. Those agencies are urged to assess ADUCT, understand its strategic impact, analyze key developments, and consequences of its ongoing growth and determine how ADUCT will evolve between today and 2030. This is essential for our national leaders to gauge the net effects of ADUCT on current defense, foreign policy, and homeland security doctrine and strategy. With that in mind, our leaders ought to assess current contingency plans and traditional security assumptions to avoid the genuine future risks of encountering unpleasant strategic surprises.

Chapter 2. Malevolent Innovation: Novelty and Effectiveness in Terror Attacks

Gina Scott Ligon
University of Nebraska Omaha
gligon@unomaha.edu

Michael K. Logan
University of Nebraska Omaha
mlogan@unomaha.edu

Creativity and Innovation in the Context of Terrorism

Terrorism provides an ideal context for examining creativity as the need for survival and innovation pervades these destructive groups. Violent extremist organizations (VEOs) operate in turbulent environments with ill-defined problems and work toward creative goals that are both ideologically and organizationally motivated. Like other types of organizations, VEOs rely on innovative solutions to achieve results and gain a competitive edge (Cropley, Kaufman, & Cropley, 2008). For example, VEOs deploy novel solutions to enhance their organizational reputation (Ligon, Harms, & Derrick, 2015), and innovative tactical and operational strategies to circumvent surveillance and scrutiny posed by adversaries (Dolnik, 2007). Few VEOs survive past the first year of their existence (Cronin, 2009); however, those that do endure because of their adaptability and innovative capacity within their environments.

One way VEOs innovate is by inventing new ways to engage in violence. More specifically, the concept *malevolent tactical innovation* (MTI) refers to inventing or adapting new methods, modes, or means of violence to achieve unchanged objectives (Crenshaw, 2000). Gill's (2017) analysis on the Provisional Irish Republican Army's (PIRA) development and usage of improvised explosive device (IED) technology illustrated that MTI varied across organizational units over a seven-year period. Although other categories of terrorist innovation exist (e.g., strategic, organizational), tactical innovation is the most heavily researched. The problem is that, despite advances, few studies have drawn from theory or methods used in traditional creativity research to examine MTI in an empirical fashion. MTI remains an underdeveloped concept.

Creativity and Innovation in the Context of Terrorism

In recent years, numerous studies examined the manifestation of creativity and innovation in the domain of terrorism (e.g., Cropley et al., 2008; Gill, 2017; Gill et al., 2013) The central premise is that, like other types of organizations, creativity is a means for VEOs to gain a competitive edge over counter-terrorism agencies as well as rival VEOs competing for resources. For example, Sinai (2015) highlights how physical and electronic surveillance and deterrence measures have inadvertently led to highly innovative counter-surveillance tactics among terrorist groups. Ligon and colleagues (2015) suggest that VEOs engage in novel acts of violence in order to enhance their organizational reputation. Together studies on creativity and innovation in the context of terrorism offer four implications. First, creativity and innovation are similar but not equal constructs. Creativity refers to the generation of novel ideas or concepts while innovation involves the implementation of these creative ideas Second, innovations is enacted through different drivers (e.g., leadership. group expertise, environment). Third, innovation can be radical or incremental. Fourth, there are three

different types of malevolent innovation in the context of terrorism, including strategic, organizational, and tactical innovation (Crenshaw, 2010). Tactical innovation occurs when terrorist organizations adopt new methods to achieve unchanged objectives. The September 11 attacks use of sequential airplane crashes as weapons and Aum Shinrikyo's use chemical weapons are exemplars of tactical innovation. The focus of the present effort is on tactical innovation because little is known as to how it manifests across a variety of terrorist attacks.

Methodology and Findings

The current study examines the dimensions and characteristics of MTI using a sample of 7,116 terrorist attacks assessed for innovation in the Leadership of the Extreme and Dangerous for Innovative Results (LEADIR; Ligon, Harris, Harms, & Friedly, 2013) project. Data for this study were content coded from attacks sampled from the Global Terrorism Database (GTD), an open-source database on terrorist events from around the world that is updated and maintained by the National Consortium for the Study of Terrorism and Responses to Terrorism (START, 2018). However, where the GTD ends and LEADIR begins is the transformation of attack level data into innovation scores from VEOs. To transform the qualitative attack data presented in the GTD into quantitative variables, we applied a coding schema used to examine other types of creative products. Specifically, eleven different variables representing the uniqueness of the weapon involved, uniqueness of the attack method, expectancy of the attack, coordination of the attack, expertise of the attack, and symbolic nature of target, scope of the attack, importance of the processes attacked, conformity to the group's ideology, furthering of the group's goal, and execution of the attack were rated on five-point Likert scales. Operational definitions with readily identifiable benchmark examples were developed for the attack-level measures of creativity and innovation. In addition, these operational definitions were defined, iteratively reviewed, and edited by a subset of subject matter experts (SMEs) on terrorist attacks (i.e., United States Special Operations Force members reviewed scales to ensure clarity, parsimony, uni-dimensionality, and relevance to the domain of terrorist attacks). This is a comparable practice to measuring innovation in Information Operations (IO) psychology, engineering, and business fields focused on the assessment of innovative products.

Research in industrial and organizational psychology suggest that innovative products include four underlying dimensions: novelty, relevance, elegance, and generalizability (Besemer & O'Quin, 1999). Of the four criteria of innovation, the results of a confirmatory factor analysis (CFA) suggest that two factors representing the *novelty* and *relevance* dimensions of MTI emerged from these data. Further analysis also suggests that the novelty dimension was related to how the attack was carried out (e.g., weapons characteristics), while the relevance dimension was related to who the attack targeted. More specifically, the novelty dimension was significantly related to sequentially linked attacks. In regard to weapons, novel attacks were significantly more likely to involve explosives and less likely to involve firearms. However, novel attacks only had small relationships (other than the moderate relationships with bombings and armed assaults with target characteristics or attack types such as assassination, hijacking, or kidnapping). Interestingly, novel attacks were significantly related to higher numbers of casualties and fatalities. Turning to the relevance dimension, no strong relationships emerged with weapon, target, or attack characteristics. This suggests that relevance is not significantly related to the attack characteristics, and this finding makes sense given that the subscales on this factor were more about the importance of the target and relevance to the group's mission. In line with other types of innovative products, it seems that MTI is driven by the strategic purpose the attack serves. Finally, relevant terrorist attacks were significantly correlated with a high number of casualties and fatalities.

Conclusions and Implications

Together our findings suggest that there are four key characteristics of MTI (i.e., attacks both high in novelty and effectiveness). The first characteristic of MTI is the use of sequentially-linked, coordinated attacks. When successful executed, a set of coordinated attacks requires more expertise and coordination, and causes more destruction as opposed to a lone incident. The second characteristic shown above is that MTI includes explosives or bombs, incendiaries, and chemical and biological weapons. Explosives or bombs and chemical or biological weapons require expertise and coordination and are highly effective when successfully deployed. Third, attacks high in novelty and relevance are more likely to target infrastructural compared to soft or high-value targets. When successfully damaged, attacks on infrastructure are higher in relevance because they are likely to have a widespread influence on important processes. Finally, hijackings and bombing events were the primary attack types associated with MTI. These attack types are also viewed as effective because, when successful executed, they further the group's goals through tangible (e.g., deaths, hostages) or other (e.g., media attention) gains.

There are at least three important implications for these findings. First, VEOs vary in their capacity for malevolent tactical innovation. Theoretically, this may mean that different antecedents drive this change in innovative performance, such as organizational resources or leadership decisions. Practically, knowing the level of MTI a VEO has shown in the past may help in allocating resources accordingly from defense and security standpoints. Moreover, MTI could provide a nice tool to guide decision makers and planners in countering non-state adversaries.

Second, this large sample dataset provides empirically supported data about VEO innovation across a variety of domains. This is the first effort to content code so many cases of terrorist attacks for the construct of malevolent tactical innovation, and the collaboration with the Special Operations Forces to ensure the ratings were valid and relevant to the operational context cannot be understated. Using large datasets such as the Global Terrorism Database (GTD; LaFree & Dugan, 2007) and the Leadership for the Extreme and Dangerous for Innovative Results (LEADIR; Ligon et al., 2013) dataset can facilitate decision making about what happens over time with innovation from VEOs.

Finally, the present effort is in line with the goal of the publication about the Third Off-Set. In order to predict and counter adversary threats, it is critical that we examine all of the possible combinations of innovation developed in the past. This particular effort can provide planners with exemplars of the highest levels of VEO innovation across a large dataset of violent extremist organizations, providing a comprehensive look at what is possible and what should be prevented.

References

Besemer, S. P. & O'Quin, K. (1999). Confirming the three-factor creative product analysis matrix model in an American Sample. *Creativity Research Journal* 12(*4), 287-296*

Crenshaw, M. (2010). Innovation: Decision points in the trajectory of terrorism. In M. J. Rasmussen & M. M. Hafez (Eds.), *Terrorist innovations in weapons of mass effect: Preconditions, causes and predictive indicators*. (p. 35-50). Washington, DC: The Defense Threat Reduction Agency.

Crenshaw, M. (2000). The psychology of terrorism: An agenda for the 21st century. *Political Psychology*, *21*(2), 405-420.

Cronin, A. K. (2009). *How terrorism ends: Understanding the decline and demise of terrorist campaigns*. Princeton, NJ: Princeton University Press.

Cropley, D. H., Kaufman, J. C., & Cropley, A. J. (2008). Malevolent creativity: A functional model of creativity in terrorism and crime. *Creativity Research Journal*, *20*(2), 105-115.

Dolnik, A. (2007). *Understanding terrorist innovation: Technology, tactics and global trends*. New York: Routledge.

Gill, P. (2017). Tactical innovation and the Provisional Irish Republican Army. *Studies in Conflict & Terrorism*, *40*(7), 573-585.

Gill, P., Horgan, J., Hunter, S. T., & Cushenbery, L. D. (20130). Malevolent creativity in terrorist organizations. *The Journal of Creative Behavior*, *47*(2), 125-151.

LaFree, G., & Dugan, L. (2007). Introducing the global terrorism database. *Terrorism and Political Violence, 19(2),* 181-204.

Ligon, G. S., Harris, D. J., Harms, M., & Friedly, J. (2013). *Organizational determinants of violence and performance: Introducing the Leadership of the Extreme and Dangerous for Innovative Results (L.E.A.D.I.R) Dataset.* Technical Report to The National Consortium for Studies of Terrorism and Responses to Terrorism (START) and The Department of Homeland Security.

Ligon, G. S., Harms, M., & Derrick, D. C. (2015). Lethal brands: How VEOs build reputations. *Journal of Strategic Security*, *8*(1-2), 27-42.

National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2018). Global Terrorism Database [Data file]. Retrieved from https://www.start.umd.edu/gtd

Sinai, J. (2015) Innovation in terrorists' counter-surveillance: The case of al-Qaeda and its affiliates. In M. Ranstorp & M. Normack (Eds.), *Understanding terrorism innovation and learning: Al-Qaeda and beyond* (p.196 -210). Abingdon: Routledge.

Chapter 3. Back to the Future: The Islamic State, Drones, and Future Threats

Don Rassler
Combating Terrorism Center at West Point
don.rassler@westpoint.edu

The Islamic State is an irony of sorts, as while the organization looks to, is inspired by, and seeks to recreate the past certain aspects of the group's behavior also provide a window into conflicts of the future. A key case study in this regard is the Islamic State's drone program, and specifically how the group "overcame technical and cost asymmetries," and creatively developed a novel and scalable drone-based weapons system "constructed from commercial components that challenged—at least for a period of time—states' ability to respond" (Rassler, 2018, p. V). As General Raymond "Tony" Thomas, the commander of U.S. Special Operations Command, noted in May 2017 "the most daunting problem [of 2016] was an adaptive enemy who, for a time, enjoyed tactical superiority in the airspace under our conventional air superiority in the form of commercially available drones and fuel-expedient weapons systems, and our only available response was small arms fire" (Larter, 2017). That accomplishment, typified by the Islamic State's successful ability to drop munitions from commercial quadcopters that had been simply modified to maim, kill, instill fear, and/or otherwise complicate operational engagements against various enemies, was no small feat.

Over the past year and a half, the scope and scale of the Islamic State's drone program has been stymied and rolled back, but it is important to not "underestimate both the organization and how the group—and its legacy of innovations—could serve as an inspiration or model for other types of actors, to include nation states or proxy groups that are developing their own hybrid warfare or asymmetric capabilities and strategies" (Rassler, 2018, p. 1). To evaluate what hostile groups or other competitors might be learning, or have learned, from the Islamic State's drone activity this paper places the group's efforts into context and identifies what was unique and noteworthy about the Islamic State's drone program. To better modulate the United States' Third Offset strategy and prepare for the future, this paper also outlines what the Islamic State's use of drones, as well as the broader trajectory of terror drone use and related proliferation, suggest about future terror and hybridized asymmetric threats. It ends with some thoughts about how the various gaps and seams that the Islamic State exploited to bring its drone program to scale could be better managed so future, related threats could be anticipated, identified, and disrupted.

Terror-Drone Evolution and the Islamic State's Contributions

Terrorist group interest in and/or use of remotely piloted aircraft, unmanned aerial systems (UAS), or "drones" is not new nor is it limited to organizations inspired by jihadist ideology (for background see Rassler, 2016). The first verified terrorism drone case occurred in 1993 when members of Aum Shinrikyo, a Japanese terrorist group inspired by apocalyptic ideology, experimented with and considered using a remote-control helicopter to distribute sarin gas to kill a rival leader in Japan (see p. 13-14, 58-60 of Rassler, 2016). Less than a decade later, in 2002, the Pakistani terrorist group Lashkar-e-Taiba leveraged a network of individuals, many of whom lived in Virginia, to acquire "sensitive technology to assist and enhance the performance" of remote-control airplanes from US companies (Rassler, 2016, p. 15-17). Two years later, in 2004, the Shia militant group Hezbollah flew a drone from southern Lebanon into Israel, and in doing so, became the first terrorist/proxy actor to fly a drone across an international border (Rassler, 2016, p. 25-29). Further, there is also evidence that terrorist groups, or individuals suspected of being motivated by terror intent, possessed and/or

used a drone in at least 12 different countries, prior to the formal establishment of the Islamic State's Caliphate in June 2014 (Rassler, 2016, p. 40-41). This included terror-drone incidents in Japan, Colombia, Iran, Iraq, Israel, Lebanon, Palestine, Pakistan, Spain, Germany, the United States, and Egypt (Rassler, 2016).

So even though the Islamic State innovated and was able to use commercially-available and homemade, Do-It-Yourself (DIY) style drones in new and unique ways, the terror-drone issue was already a fairly well-proliferated problem with interest being shown by geographically distributed terror entities before June 2014 (Rassler, 2016). Thus, the Islamic State drone threat is arguably best understood not as some type of entirely new development, but rather as a new iteration of a specific terrorist interest area with two and a half decades worth of history. This "view-of-the-problem" distinction is important as it has a bearing on: 1) how current terror, and other hybridized, threats that leverage—and are built around—commercial-off-the-shelf technologies are situated, and 2) how future iterations of those type of threat steams, including those perpetrated by terrorists, proxy groups, states, and individual citizens, are modeled, tracked, and managed in relation to the Third Offset context.

To do the latter well and reduce the risk of strategic surprise, it is important that the history and context of specific threat streams be outlined, that key innovation points and creative use cases of specific technologies be identified, and that the current, operational state of the art of various technologies (including the capabilities and potential disruptive impacts of soon-to-be emerged technologies) be clearly defined for planners and strategists. An unpacking of some of these elements in relation to the Islamic State's drone innovations is provided to illustrate the utility of taking a broader, non-group based functional threat stream approach, especially when the threat leverages commercial systems.

When the history of terror-drone interest and use cases that occurred prior to the Islamic State's formal declaration of its Caliphate in June 2014 are evaluated, five important and concerning focus areas stand out.

1. First, is the early interest of Aum Shinrikyo in using drones as a platform to deliver chemical and biological agents; an interest which was observed again in 2013 when the first traces of the Islamic State's drone activity came into public view (see Rassler, 2016, p. 13-14, 34-35, 58-60). This issue takes on enhanced significance given the Islamic State's repeated use of chemical weapons in Syria (Rassler, 2018; Gibbons-Neff, 2016) and the disruption of several chemical and biological terrorist plots linked to the group over the last two years (for background see Zammit, 2017; Fade, 2018; Rachman, 2017) including a "very serious" ricin plot thwarted in Germany in June 2018 that involved the discovery of over 3,000 castor beans and 84.3 milligrams of ricin (Rassler, 2018, p. 21-22; Cruickshank, 2018; Cologne Ricin Plot Bigger Than Expected, 2018). The various recent state chemical weapon use cases, as typified by the Russian-linked Novichok poisoning incident in the United Kingdom (Cruickshank, 2018; Smith-Spark & Veselinovic, 2018), the Assad government's use of chemical weapons in Syria ("Timeline of Syrian chemical weapons activity", 2018), and the assassination of the half-brother of North Korean leader Kim Jong Un in Malaysia with VX nerve agent by North Korean-linked operatives, further complicates the chemical-biological weapons threat picture—especially since the nations tied to these events are hostile to or do not have good relations with the United States (Ma, 2018). These data points reveal how the potential use of drones as a future chemical-biological delivery mechanism for non-state and state actors is a critical threat vector that must be monitored.

2. Second, is terror-group use of drones for cross-border missions—a precedent first set by Hezbollah in 2004 and that the organization has repeated on a number of occasions (Rassler, 2016, p. 26). Given the defensive measures Israel has put in place, it is now harder for Hezbollah to conduct these types of missions, but Hezbollah's cross border drone flights into Israel are noteworthy as they demonstrate a capability to fly and control drones at range—a capability that almost certainly has been aided by Hezbollah's close relationship with Iran and the more-sophisticated drone technology to which it has had access. Autonomous flight control/programming features, enhanced battery power, and lighter commercial drones will provide proxy and non-state actors with the ability to fly their drones further from their controllers in the future. One example that demonstrates what future extended range capabilities could look like is "Maynard Hill's successful flight of a commercially modified UAS across the Atlantic Ocean, a feat that he and his team achieved in 2003 with an 11-pound UAS, an autopilot system and less than a gallon of gas" (Rassler, 2016, p. 46). As previously noted by the author, "Hill and his team *were* experienced UAS hobbyists, but their feat illustrates that there are ways to leverage commercial technology to significantly extend a [drone's] range" (Rassler, 2016). And with added range comes new threat possibilities, including opportunities to attack targets from considerable stand-off distances or to launch drone attacks from harder-to-reach locations (which might make it harder for local authorities to stop the event or find the perpetrators).

3. Third is terror-group desire to weaponize remote-control aircraft and drone platforms. In 2005, the Secretary General of Hezbollah, Hassan Nasrallah, boasted that the group's drones could be "packed with 40–50 kg of explosives" and be used "to attack priority targets deep inside Israel" ("Israel Intercept Two Attack UAV", 2006). The next year, Hezbollah is reported to have flown an explosive-laden drone into Israel, which Israeli Defense Forces downed (Burke, 2010). The case is noteworthy because it "represented the first successful attempt by a terrorist group to load a conventional weapon onto a UAS" (Rassler, 2016, p. 27).[1] Two years later a private citizen in the United States mounted a handgun to a modified commercial-off-the-shelf remote-control helicopter and successfully fired the weapon (for background see Rassler, 2016, p 55-57). And he did so not to support a terrorist objective, but to demonstrate that such an action was possible. These incidents were followed by disrupted drone weaponization terror plots in the United States in 2011 (see Rassler, 2016, p. 19-22) and in Germany in 2013 (for background see "Two men investigated in Germany", 2013; Ney, 2013).[2] It is much easier to weave these cases together with the benefit of hindsight, but these data points also highlight how attaching explosives to, or mounting a weapon onto, a drone (including commercial versions) had been an objective for several terrorist actors for a considerable period of time before the Islamic State developed its drone bomb-drop capability.

4. Fourth, is the existence of resourced drone programs run by at least two terror-linked groups, Hezbollah and HAMAS—prior to Islamic State's Caliphate announcement in June 2014. Indeed, before that date these two groups had "either used drone frequently enough, or [had]… identifiable mid-to-long term infrastructure dedicated to supporting such operations, that their efforts warrant being labeled as a 'program'" (Rassler, 2016, p. 13). The subsequent development of the Islamic State's drone program (and the existence of a smaller program effort run by Hayat

[1] Initial point made by Burke (2010). As the author has previously noted: "It is still not clear if the attempt by Aum Shinrikyo should be considered the first attempt to weaponize a UAS, even though the group potentially weaponized its remote-control helicopter with unconventional weapons. There is a need for additional information to firmly establish this point." See Rassler (2016, FN 172).

[2] There is a discrepancy between these two sources, as one mentions that the Tunisian students were investigated, while another says they were arrested. See also Nicas (2015).

Tahrir al-Sham) makes it all the more important that Third Offset planners and strategists recognize that the drone actions of some terror groups are not a series of one-off events, but rather a more "structured, integrated and resourced capability" (Rassler, 2016), features which have a bearing on the sophistication and endurance of the threat. A related challenge is that the Islamic State and Hayat Tahrir al-Sham have developed their programs through the repurposing and creative cobbling together of commercially-available systems and components that they have been able to acquire; a dynamic which poses unique detection and disruption challenges.

5. Fifth is the ability of several terror groups to either gain access to drone feeds or to hack drones operated by nation states. This includes Hezbollah's ability to gain access to Israeli drone feeds in 1997, Kataib Hezbollah's interception of data from US drones operating in Iraq in 2009, and the ability of a Palestinian Islamic Jihad activist to hack Israeli drones in 2016 (for background on the Hezbollah case and Palestinian Islamic Jihad activist case, see Rassler, 2016, p. 25, 34; for background on Kataib Hezbollah example, see Rassler, 2017). These cases illustrate how actions by terror groups to identify and exploit security gaps and seams occur across a range of offensive and defensive fronts. These incidents are also a useful reminder that the drone, counter drone competition that is "being played out between the United States and its adversaries" is an iterative cat-and-mouse game that will continue to evolve (Rassler, 2017).

So, if all of these things had already occurred before the Islamic State and its drone-bomb drop capability exploded onto the scene what, if anything, makes what the Islamic State achieved with drones significant or unique. Two factors stand out in this regard. To start, the Islamic State is the first known terror group that used a drone, especially a commercially-available device, to kill. The second factor that is new and makes the Islamic State's drone program stand out is that the group was able to source, assemble, deploy, and make successful use of a fleet of creatively modified commercially available drones (and in some cases homemade drones) and do so at scale. The group's ability to source as many quadcopter drones as they did was "underpinned and facilitated by the group's ability to acquire commercial quadcopter drones and related components… through a global and layered supply chain that involved purchases from at least 16 different companies that were based in at least seven different countries" (Rassler, 2018, p. IV). Different purchasing networks facilitated these various transactions. For example, according to the U.S. Treasury Department Yunus Sakarya, an individual operating out of Turkey, "was involved in transactions for UAV [Unmanned Aerial Vehicle]-related equipment that totaled over $500,000 for ISIS," (US Department of Treasury, 2018) while other Islamic State drone purchasing networks operated from and used front companies based in the United Kingdom, Spain, Denmark, and Bangladesh (for background see Rassler, 2018; Atherton, 2018; Larsen, Dalsgaard, Myli Albæk, & Vithner, 2018). And it appears that many of these transactions were made from online retailers based in places like the United States, Canada, and Denmark by third parties who were either working with or on behalf of the Islamic State (see Rassler, 2018; Atherton, 2018; Larsen, Dalsgaard, Myli Albæk, & Vithner, 2018). The irony of course is that Islamic State operatives often acquired commercial technology sold in the West—and in other areas outside of its Caliphate—to aid its fight against Western nations, the Iraqi government, the Syrian regime, and uncooperative civilians in the Levant.

Given the relatively low cost of the drones the Islamic State used and the ease with which those and other similar forms of dual-use technology can be purchased (and repurposed), there is a danger that other hostile actors, to include near-peer competitors, will look at the Islamic State's drone program as a component or model that could be used to augment or enhance their existing capabilities or asymmetric warfare strategies. While the scale of the Islamic State drone threat has been rolled back, the group's experience with drones is also instructive as it shows how threats that leverage and are built around dual-use technologies can be used to surprise—and that they represent an important

and exploitable security gap. Due to their dual-use nature these types of threats are difficult to detect, monitor, and prevent. Another important take-away from the Islamic State's drone effort is that these types of threats might not even be noticed or effectively countered before a significant threat capability has been developed and scaled.

Conclusion

The Islamic State's drone accomplishments speak to, and have a number of important implications regarding, the character and style of future threats that are either constructed around or that significantly leverage dual-use commercial technologies —and how other, similar types of dual-use technology derived threats might be better mapped and detected.

As we prepare for the future, attention should be placed on the five historical terror-drone focus areas that preceded, and were made even more significant by, the Islamic State's interests and drone-related capabilities. The terror drone threat will evolve and we should expect: 1) drones similar to the Islamic State's bomb-drop capable ones to be used in different areas by different groups, including those motivated by different ideologies; 2) the creative use of commercial systems (to include the future use of autonomous control technologies, likely pared with other technologies) to develop new drone threat tactics and weapons—so new targets can be struck; and 3) more commercial drones to be used in nefarious ways by terrorists: not just a single drone, but multiple drones, and sea and land drones too (Rassler, 2018, p. 19-23).

To stay ahead of the issue, and to better prepare for a future that will almost certainly be typified by the proliferation of other hybrid threats that leverage and/or repurpose commercial systems in dangerous ways, the United States should identify the pathways and methods that allowed the Islamic State to acquire and scale its fleet of quadcopter drones in the first place. It is true that terrorist groups and "hostile state actors will almost always be able to find supply chain gaps and seams" (Rassler, 2018, p. 24). But, as the author has noted previously, "that does not mean that efforts cannot or should not be made to tighten or better track the purchase of predictable dual-use items—such as commercial drones, rocket and counter-surveillance equipment, and other similar devices that helped the Islamic State to enhance its defensive and offensive capabilities—through creative partnerships with industry" (Rassler, 2018).

References

Atherton, K. (2018, September 28). Is ISIS buying valuable military equipment in Western Europe? In *C4ISRNET*. Retrieved from https://www.c4isrnet.com/unmanned/2018/09/28/arrests-in-denmark-suggest-isis-still-has-drone-buyers-in-europe/

Burke, P. (2010). *The terrorist threat to the maritime security of the UAE.* Emirates Center for Strategic Studies and Research, Emirates Lecture Series No. 85.

Cruickshank, P. (2018). A view from the CT foxhole: An interview with Hamish de Bretton-Gordan, former Commander of the U.K. CBRN regiment. *CTC Sentinel, 11*(7), 5-9.

Cologne ricin plot bigger than expected. (2018, June 6). *Deutsche Welle.* Retrieved from https://www.dw.com/en/cologne-ricin-plot-bigger-than-initially-suspected/a-44319328

Fade, F. (2018). The June 2018 Cologne ricin plot: A new threshold in jihadi bio terror. *CTC Sentinel, 11*(7), 1-4.

Gibbons-Neff, T. (2016, November 22). Report: Islamic State has used chemical weapons 52 times in Iraq and Syria since 2014. *Washington Post*.

Israel intercept two attack UAV launched by Hezbollah (2006, August 14). *Defense Update*.

Larsen, T. K., Dalsgaard, L., Albæk, M. M., & Vithner, J. (2018, September 27). Tidligere amerikansk terrorchef: Basil Hassan er en af de farligste på vores terrorliste. In *DR*.

Larter, D. (2017, May 17). SOCOM Commander: Armed ISIS drones were 2016's 'Most Daunting Problem.' *Defense News*

Ma, A. (2018, February 13). Kim Jong Un's half-brother was assassinated with nerve poison one year ago — here's how it went down and the remaining unsolved mysteries. *Business Insider*.

Ney, J. P. (2013, October 15). Terrorist drones: States are taking steps," In *Infosdefense.com.*

Nicas, J. (2015, January 29). Criminals, terrorists find uses for drones, raising concerns. In *Wall Street Journal*.

Rachman, A. (2017, August 16). Chemical bomb plot inspired by Islamic State: Indonesian Police. *Wall Street Journal*.

Rassler, D. (2016). *Remotely piloted innovation: Terrorism, drones and supportive technology*. Combatting Terrorism Center. Retrieved from https://ctc.usma.edu/app/uploads/2016/10/Drones-Report.pdf

Rassler, D. (2017). Drone, counter drone: Observations on the context between the United States and Jihadis. *CTC Sentinel, 10*(1), 23-27.

Rassler, D. (2018). *Islamic State and drones: supply, scale, and future threats.* West Point, NY: Combating Terrorism Center.

Smith-Spark, L. & Veselinovic, M. (2018, September 5). Russians charged over UK Novichok nerve agent attack.

Timeline of Syrian chemical weapons activity, 2012-2018. (2018). In *Arms Control Association*.

Two men investigated in Germany over alleged terror plot using model planes. (2013, June 25). In *Daily Mirror*.

US Department of Treasury (2018, February 9). *Treasury sanctions ISIS facilitators across the globe*. [Press Release]. Retrieved from https://home.treasury.gov/news/press-release/sm0284

Zammit, A. (2018). New developments in the Islamic State's external operations: The 2017 Sydney Plane Plot. *CTC Sentinel, 10*(9), 13-18.

Chapter 4. Exploring Pro-Islamic State Instructional Material on Telegram

Bennett Clifford
Program on Extremism, George Washington University
bennettclifford@gwu.edu

Key Points

- English-speaking supporters of the Islamic State use the messaging application Telegram to distribute a range of information, including instructional material—manuals and guides designed to aid operatives with step-by-step procedures for providing assistance to the group.
- Channel administrators distribute whichever manuals they believe can be of aid to aspiring operatives, regardless of its ideological background.
- Telegram's internal file-sharing features and lax approach to content moderation allow channel administrators to create repositories of instructional information within Telegram channels.
- While attack-planning manuals available on Telegram channels understandably pose a large concern for counterterrorism authorities, operational security and cybersecurity manuals are also frequently distributed, relatively easy to implement, and help operatives successfully conduct activities in support of terrorist groups while minimizing the risk of detection or apprehension.

Abstract

Online, English-speaking supporters of the Islamic State utilize the messaging application Telegram not only to communicate internally and distribute the group's media and propaganda products, but also have utilized the platform to share instructional material. In basic terms, instructional material refers to compiled, published, and disseminated information about how operatives can assist terrorist groups successfully and inconspicuously. Researchers reviewed 98 pro-Islamic State Telegram channels, collected between June and December 2017. The resulting analysis found that administrators of these channels shared a plethora of instructional material from inside and outside the jihadi movement, that the use of Telegram fundamentally changed the nature of instructional material distribution, and that while attack-planning manuals understandably concern counterterrorism authorities, manuals documenting operational security and cybersecurity protocols are arguably of equal concern (Clifford, 2018).

Methodology

The 98 channels analyzed in this study represent 16.2% of the Telegram channels collected by researchers at the Program on Extremism from June to December of 2017 (For more information on the methodology behind Telegram channel collection, see "About the Telegram Tracker"). The channels had an average of 98.7 members per channel, with the most-followed channel boasting over 350 members. Across these channels, supporters shared over 7,560 photos, 536 videos, 300 audio messages, 8,243 files, and 689 URL links ("About the Telegram Tracker"). Within these channels, three types of material were most prominent:

- **Explosives construction**: information and step-by-step instructions to synthesize explosive material, improvised explosive devices, and instructions for carrying out an attack using explosive devices
- **Low-tech attacks**: information and guidance about conducting attacks that do not require explosive devices (knife attacks, vehicular assaults and rammings, arsons, train derailments, etc.)
- **Operational security and cybersecurity**: information about avoiding detection while implementing a plot and reducing the risk of apprehension; instructions to avoid monitoring of online activity, including the installation of privacy-maximizing applications and services (virtual private networks, anonymous browsers, 'self-destruct' features, encrypted messaging and e-mail services, etc.)

Instructional material and the "a la carte" approach to jihadi attack planning

The first major finding of this study is that administrators of pro-ISIS Telegram channels that distribute instructional material are less discerning about the organizational source of the material that they post, and that they frequently use material from outside the narrow confines of ISIS-produced material. Three factors—the dearth of officially-produced ISIS instructional material, the surfeit of material produced by other groups, and English-speaking jihadis' seeming inability to discern between sources—all encourage English-language, pro-Islamic State Telegram channel administrators to post instructional material from inside and outside the jihadi movement. In the context of instructional material, rigidity to the ISIS "brand" does not seem to be required. Within this study's sample, channel administrators not only shared material from ISIS, but also from ISIS' jihadi competitors and rivals, as well as from non-jihadi sources like declassified military manuals, "disaster prepper" guides, and crowd-sourced cybersecurity tips (Clifford, 2018).

The depth of instructional literature produced by other jihadist groups is an asset for English-speaking attack planners. Previous studies explored a vast collection of English-language jihadi instructional material distributed online by other groups, which remain influential today (Conway, Parker, & Looney, 2017; Reed & Ingram, 2017). Of greatest notoriety are perhaps the e-magazines of al-Qaida in the Arabian Peninsula (AQAP), in particular its flagship publication, *Inspire* (Conway, Parker, & Looney, 2017; Reed & Ingram, 2017). *Inspire,* among other recurring series, included the now-infamous *Open Source Jihad* section. This section contained instructional manuals for a variety of attacks, including car bombings, vehicular attacks, and improvised explosive device (IED)-based attacks. It also contained instructions for an encrypted messaging protocol and other cybersecurity instructions (Lemieux, Brachman, Levitt, & Wood, 2014). Nearly ten years after AQAP released the first issue of *Open Source Jihad* in 2010, English-speaking jihadis around the world continue to utilize instructions contained therein (Sarat-St. Peter, 2017).

In contrast, the amount and diversity of existing, officially-produced, English-language ISIS instructional material pales in comparison to the group's rivals. A 2017 study by Ingram and Reed found that ISIS did not publish instructional material in the 15 issues its first official English-language publication, *Dabiq*, and in its second English release, *Rumiyyah,* only five out of 13 issues to date contain instructional material (Reed & Ingram, 2017). These five issues of *Rumiyyah* contain ISIS' "answer" to *Open Source Jihad*, which it calls *Just Terror Tactics.* Notably, *Just Terror Tactics* eschews instructions for plots that require extensive planning, resources, or expertise, focusing on small-scale, low-budget attacks like stabbings, vehicular rammings, or arson (Reed & Ingram, 2017). This mirrors the group's external operations strategy, which, in its assessment that directing low-tech attacks can result in strategic gains and minimal losses if the attacker is disrupted, aims to push

supporters that cannot travel to receive training with the group to immediately attack at home with whichever methods are available to them (Reed & Ingram, 2017).

Nevertheless, a dilemma occurs when would-be English-speaking ISIS supporters are still interested in high-casualty, resource-intensive attacks, especially those involving explosives. In December 2017, Akayed Ullah detonated an IED based loosely on instructions from "Make a bomb in the kitchen of your mom," an explosives-construction manual from *Open Source Jihad* (Weiser & Palmer, 2018). Despite utilizing the instructions from ISIS' competitor AQAP, which he found online, Ullah later admitted to investigators that he had declared allegiance to ISIS and consumed other pro-ISIS propaganda (Weiser & Palmer, 2018). In this case, in addition to several other notable ISIS-affiliated attackers in the United States, Ullah drew succor not only from the strictly-defined propaganda material of ISIS, but also from material produced by its rivals. In achieving the objective of a successful attack, English-speaking attack planners have been found to be especially likely to employ an "a la carte" approach to jihadist propaganda and ideology, selecting the details from each movement that are personally relevant to them (Hegghammer & Nesser, 2015; Vidino, Marone, & Entenmann, 2017; Pascarelli, 2016).

Telegram's unique file-sharing features, as well as the company's approach to content moderation, shape its use as a platform for the sharing of jihadi media. Prucha described ISIS' use of Telegram as an "information highway" used to coordinate a "multiplatform zeitgeist," wherein Telegram channel administrators share media produced by the group's central media authorities, and then supporters blend it with unofficial propaganda, commentary, and other information (Prucha, 2016). Continuing the chain of dissemination, supporters distribute this blend of material onto public-facing social media sites (e.g. Facebook, Twitter, YouTube, Instagram) and filesharing platforms (e.g. Internet Archive, Justpaste.it, Google Drive) (Prucha, 2016). Previous studies mainly focused on ISIS' use of Telegram to spreading media products and propaganda (Prucha, 2016; Bloom, Tiflati, & Horgan, 2017; Shehabat, Mitew, & Alzoubi, 2017). This study, which focused on instructional material specifically, found that two Telegram features represented significant assets to supporters and channel administrators in sharing this unique content.

First, Telegram's internal filesharing capabilities far outstrip other platforms that are popular within the online jihadisphere. Within a channel, users can share individual files of up to 1.5GB ("Shared Files and Fast Mute", 2015). Telegram supports a number of media uploads, including video, audio, photo, documents, and voice messages ("Shared Files and Fast Mute", 2015). In contrast, Twitter, another preferred platform for English-speaking ISIS supporters, can only support photo and video uploads of up to 512MB ("Upload Media"). Outside of Telegram, supporters are often forced to share large files or non-supported file types using external filesharing sites. Using external sites, very few of which offer encryption or a guarantee against content takedowns, is a much riskier choice. By storing content on Telegram, instead, ISIS supporters can generate "clearinghouses" of content and a steady platform for housing material before its eventual upload onto the surface web (Clifford, 2018).

In addition, Telegram is generally slower than other companies to implement Terms of Service (ToS) enforcement that target jihadist exploitation of the platform. Under pressure, the company cites free speech concerns, and claims that governments overestimate the degree and impact of ISIS material shared on its site (Ra, 2017; Bohlen, 2017). While it operates a channel, named "ISIS Watch," that tracks the number of channels it takes down daily, monthly, and yearly for terrorism-related ToS violations, its methodology for determining which channels cross the threshold is opaque ("ISIS Watch"). Nevertheless, ISIS supporters have already devised methods for circumventing takedown procedures. For instance, an administrator of a channel will upload all media to a "master" channel with no followers, create several more, and then forward the media to the newly-created channels.

As the channels gain followers, the chances of their takedown increase, but the administrator always has access to the seed channel and can use it to generate multiple iterations of the same channel.

Telegram has revolutionized jihadi online instructional material distribution by combining extensive file-sharing capabilities in multiple file formats with lax regulation. Administrators of pro-ISIS Telegram channels use the platform's array of file compatibilities to distribute video, audio, document, and photo versions of instructional manuals. This partially inoculates the material from detection by algorithms that are trained to only analyze one type of file for malicious content and ensures that supporters can store instructional material within Telegram channels with limited fear of takedowns or suspensions.

Potential impacts of online ISIS instructional material

Despite the wide-reaching availability of several operational guides for terrorist attack planners available on ISIS and other jihadi Telegram channels, accessing this material may not always lead to improved chances of attack success. For all terrorist instructional material, online or offline, there remains a distinction between *techne* (having the general information or knowledge necessary to perpetrate a terrorist attack) and *metis* (having hands-on training or previous experience in specific methods) (Kenney, 2010). The *techne* of an online manual will never be an effective substitute for *metis* attained through direct, in-person training. This gap becomes more pronounced as the scale of the planned attack increases, especially if it involves explosives construction. Would-be ISIS-affiliated attackers throughout the Western world, notably in New York, Barcelona, and Brussels, failed to assemble working explosive devices, synthesize explosive material, or successfully detonate their devices, which they developed in many cases from instructional material (Kenney, 2010).

Further studies are necessary to discern the impact of instructional material on lower-budget attacks that do not involve the use of an explosive device. However, the operational security and cybersecurity manuals available on pro-ISIS Telegram channels should be of immediate concern to counterterrorism authorities in the West. This type of instructional material, found on over 70% of the channels surveyed in this study, can abet attack planners by helping them avoid efforts by law enforcement to interdict and disrupt their plots. Moreover, in comparison to attack-planning guides, OPSEC and cybersecurity manuals are easier for individuals without specialized knowledge to implement. While following the instructions contained in these manuals may not directly result in casualties, they can act as "force multipliers" by decreasing the risk that operatives are apprehended before successfully carrying out their plots.

Moreover, the cybersecurity instructions available on pro-ISIS Telegram channels also have implications for preventing the spread of extremist material on mainstream, public-facing websites. Telegram's internal filesharing features allow supporters access to a nearly-uninterrupted base of material that they can constantly re-upload onto major social media and external filesharing sites. Following certain manuals also grants them the ability to proliferate email accounts, as well as corresponding Facebook, Twitter, and Google accounts. Through this process, individual ISIS supporters guarantee that in the event of account suspension or takedown, they have several other accounts on each site that they can fall back on. This severely complicates the efforts of major service providers to detect and remove all extremist content, including instructional or operational guides, from their platforms.

Overall, the dearth of officially-produced ISIS instructional material in the English language is no guarantee that English-speaking supporters of the group will be uninterested in committing attacks in their home countries, even despite the group's rapid loss of territory in Syria and Iraq. The expanse

of unofficially-produced material and strategic borrowing from other instructional material, however, is an indicator of how ISIS supporters will continue to spark attack plots in lieu of territorial and organizational deficits. Understanding the full scope of what types of material are available will be vital to forthcoming efforts to identify and intercept future ISIS-inspired attack plots in English-speaking countries, including in the United States.

References

Bloom, M., Tiflati, H., & Horgan, J. (2017). Navigating ISIS's preferred platform: Telegram. *Terrorism and Political Violence*, 1–13. Retrieved from https://doi.org/10.1080/09546553.2017.1339695

Bohlen, C. (2017, December 21). Does the messaging service Telegram take privacy too far? *The New York Times*. Retrieved from https://www.nytimes.com/2016/09/06/world/europe/telegram-isis-privacy-encryption.html

Clifford, B. (2018). Trucks, knives, bombs, whatever: Exploring Pro-Islamic State instructional material on Telegram. *CTC Sentinel*, 11(5). Retrieved from https://ctc.usma.edu/trucks-knives-bombs-whatever-exploring-pro-islamic-state-instructional-material-telegram/

Conway, M., Parker, J., & Looney, S. (2017). Online Jihadi instructional content: The role of magazines. In M. Conway, L. Jarvis, O. Lehane, S. Macdonald, & L. Nouri (Eds.), Terrorists' Use of the Internet: Assessment and Response. Amsterdam: IOS Press

Hegghammer, T., & Nesser, P. (2015). Assessing the Islamic State's commitment to attacking the West. *Perspectives on Terrorism, 9*(4). Retrieved from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/440

"ISIS Watch." Telegram channel. Retrieved from https://telegram.me/ISISwatch

Kenney, M. (2010). Beyond the Internet: Mētis, Techne, and the limitations of online artifacts for Islamist terrorists. *Terrorism and Political Violence,* 22(2), p. 177–197. Retrieved from https://doi.org/10.1080/09546550903554760

Lemieux, A. F., Brachman, J. M., Levitt, J., & Wood, J. (2014). Inspire Magazine: A critical analysis of its significance and potential impact through the lens of the information, motivation, and behavioral skills model. *Terrorism and Political Violence, 26*(2), 354–371. Retrieved from https://doi.org/10.1080/09546553.2013.828604

Pascarelli, P. (2016, October 2). Ideology à la carte: Why lone actor terrorists choose and fuse ideologies. https://www.lawfareblog.com/ideology-%C3%A0-la-carte-why-lone-actor-terrorists-choose-and-fuse-ideologies

Prucha, N. (2016). IS and the Jihadist information highway – projecting influence and religious identity via Telegram. *Perspectives on Terrorism, 10*(6). Retrieved from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/556

Reed, A., & Ingram, H. (2017). Exploring the role of instructional material in AQAP's Inspire and ISIS' Rumiyah. The Hague: Europol. Retrieved from https://icct.nl/wp-content/uploads/2017/06/reeda_ingramh_instructionalmaterial.pdf

Sarat-St. Peter, H. A. (2017). Make a bomb in the kitchen of your mom: Jihadist tactical technical communication and the everyday practice of cooking. *Technical Communication Quarterly, 26*(1), 76–91. Retrieved from https://doi.org/10.1080/10572252.2016.1275862

"Shared Files and Fast Mute" (2015, February 2). Telegram. Retrieved from https://telegram.org/blog/shared-files

Shehabat, A., Mitew, T., & Alzoubi, Y. (2017). Encrypted Jihad: Investigating the role of Telegram app in lone wolf attacks in the West. *Journal of Strategic Security, 10*(3). Retrieved from https://doi.org/10.5038/1944-0472.10.3.1604

"Telegram Tracker- Fall 2017." Program on Extremism. Retrieved fromhttps://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Telegram%20Tracker%20Fall%202017%20%285%29.pdf

"Upload Media." Twitter Developer. Retrieved from https://developer.twitter.com/en/docs/media/upload-media/overview

Vidino, L., Marone, F., & Entenmann, E. (2017). Fear thy neighbor: Radicalization and Jihadist attacks in the West (ICCT-Program on Extremism-ISPI Report). Retrieved from https://icct.nl/wp-content/uploads/2017/06/FearThyNeighbor-RadicalizationandJihadistAttacksintheWest.pdf

Weiser, B., & Palmer, E. (2018, November 7). Akayed Ullah guilty of ISIS-inspired bombing near Times Square. The New York Times. Retrieved https://www.nytimes.com/2018/11/06/nyregion/port-authority-bombing-verdict.html

Ra, M. (2017, March 27). Don't shoot the messenger. Telegram. Retrieved from https://telegra.ph/Dont-Shoot-the-Messenger

Chapter 5. Examining the Present and Future Role of Cybercrime-as-a-Service in Terror and Extremism

Thomas J. Holt
School of Criminal Justice, Michigan State University
holtt@msu.edu

Abstract

The rise of online illicit markets that enable the sale of cybercrime tools and stolen personal information have made it possible for individuals to engage in technically sophisticated forms of crime regardless of level of computer skill. Ideological and terror groups over the last decade have expressed an interest in cyberattacks as a means to cause harm, though it is not clear how much ability they have to perform such attacks. As a result, cybercrime markets may engender their attacks, though it is not clear how often this may occur, or what conditions would lead to their use. This document provides recommendations for policy and research to disrupt cybercrime markets and improve our knowledge of ideologically-motivated cyberattackers generally.

Cybercrime markets generate millions of dollars in revenue and enable non-technical actors to perform sophisticated attacks. They may provide a point of entry for ideologically-motivated extremists and terrorists to engage in cyberattacks. These markets can be disrupted through traditional law enforcement investigations, and may also be affected through other extra-legal efforts such as Sybil attacks. Research is needed on the radicalization process of ideologically-motivated actors who engage in cyberattacks, and how this differs from those who have engaged in physical attacks.

Understanding Cyberattacks and Cybercrime-As-Service Markets

Over the last two decades there has been a substantial increase in the number of cyberattacks affecting civilian, governmental, and industrial targets. A portion of these attacks stem from nation-state-sponsored actors, who are funded either whole or in part by military or government organizations (Andress & Winterfeld, 2013; Brenner, 2010; Holt & Bossler, 2016). Though such incidents are now part of the broader use of cyberspace as a military operational space, a much larger portion can be attributed to non-nation-state actors motivated primarily by economic gain (Ablon, Libicki, & Golay, 2014; Holt & Bossler, 2016; Wall, 2007).

Many of these attacks involve attempts to compromise financial institutions, retailers, and organizations to acquire sensitive financial data which can be resold to others for use in fraud and theft (Ablon et al., 2014; Holt, & Lampke, 2010; Motoyama, McCoy, Levchenko, Savage, & Voelker, 2011). These online markets operating via forums and shops enable vendors and buyers to earn millions of dollars annually based around the sale of credit card numbers, bank account details, and other financial information (Holt, Smirnova, & Chua, 2016; Franklin et al., 2007; van Hardeveld, Webber, & O'Hara, 2017). There is also a range of illicit services that can be used to further monetize personal information through the use of online purchasing services and goods processors, money transfers, and other tools (Motoyama et al., 2011; van Hardeveld et al., 2017). There are also a number of actors who produce malicious software and attack tools which can be used for various

purposes, ranging from computer intrusions to distributed denial of service attacks that render data and services inoperable (Dhanjani & Rios, 2009; Holt, 2013; Holz, Engelberth, & Freiling, 2009; Hutchings & Clayton, 2016; Karimi & McCoy, 2013).

The growth of this illicit economy is arguably due to the massive profits that buyers and sellers may generate from participating in the market (Holt et al., 2016; Moore, Clayton, & Anderson, 2009). The scope of the market may also be a function of its power as a leveling factor in cybercrime—sellers provide access to user-friendly tools and data that enable anyone to engage in attacks regardless of their level of skill (Franklin et al., 2007; Holt, 2013). Vendors also note the technical expertise needed to operate their tools, and typically operate customer service and technical support contact lines to ensure their products can be used (Ablon et al., 2014; Holt & Lampke, 2010).

The persistence of cybercrime markets begs the question as to why extremists and ideologically motivated actors do not utilize these resources to engage in cyberattacks. To date, there is generally little empirical research demonstrating the use of cyberattacks by ideologically motivated actors and terror groups (e.g. Holt et al., 2017; Jordan & Taylor, 2003). Additionally, there is limited anecdotal evidence of terrorists involvement in stolen data markets for fundraising purposes (Peretti, 2009), and successful attacks stemming from tools or techniques available from cybercrime markets (DHS, 2009).

The lack of attacks may be a result of limited technical expertise or perceived value in cyberattacks compared to physical attacks (Holt & Bolden, 2014). For instance, far right groups in the US appear to have limited technical capacity beyond social media manipulation (Holt & Bolden, 2014). Participants in far left groups may, however, be more inclined toward cyberattacks because of their educational and employment experience, as well as their interest in economic harm against industry and government targets (e.g. Freilich et al., 2014). In fact, the U.S. Department of Homeland Security (2009) argued that there would be an increase in cyberattacks performed by far-left extremist groups over the next decade. Similarly, jihadist groups have actively recognized the utility of cyberattacks against western targets to cause economic harm and reduce trust in government agencies (Britz, 2015; Denning, 2011).

As a result, it is possible that cybercrime markets may become a resource in the attack arsenal of ideological groups in the near future. In order to reduce the potential for these markets to facilitate cyberattacks by ideological and terrorist actors, there is a need to proactive identify disruption and intervention strategies that may impact both the cybercriminal community and ideological actors.

First, there is a need for increased investigations into cybercrime economies and attempts to engage in large scale disruption via forum takedowns and arrests (Hutchings & Holt, 2017). The use of multi-national investigations that lead to the arrest of key players, particularly forum managers, is vital to reduce confidence in the legitimacy of forum operations and market actors. This kind of investigation is extremely time- and resource-intensive, which may limit its utility in the short term. Additionally, many of these forums are populated in part by Russian actors with no likelihood of extradition in the event of an indictment (Brenner, 2010). Legal action may, however, cause the majority of participants who are unaffected by arrest to displace to other markets operating on more protected platforms (Holt & Lampke, 2010; Hutchings & Holt, 2017). This effort may make it difficult for ideological actors to gain access to the forums which increases barriers to entry and complicates the offending process (Holt & Bossler, 2016).

Extralegal options may also be employed to complicate the process of buying and selling products within cybercrime markets. Since many of the markets operate through clear-text advertisements for products, individuals interested in buying a good or service may be overwhelmed by the quantity of vendors. The range of options leads customers to typically seek information on the legitimacy of a vendor and the quality of their products prior to making a purchase. Customer feedback through product reviews serves as the primary point of information to assess vendor competency. As a result, researchers have argued in favor of the use of slander attacks, where forums are flooded with false reviews and feedback from spam accounts in an attempt to sow confusion and complicate the decision-making process for buyers (e.g. Franklin et al., 2007; Holt & Lampke, 2010; Hutchings & Holt, 2017). Such efforts may be useful to help disrupt illicit market operations and complicate the process of buying and selling for novice users and known actors alike.

In addition to legal efforts, there is a need for empirical research to develop insights into the technological skills and capacities of extremist and terror groups to successfully complete cyberattacks (Britz, 2015; Holt & Bolden, 2014; Weimann, 2011). It is unclear what proportion of extremist groups and terrorist networks have sufficient knowledge of computer hardware and software to engage in attacks at present, or their baseline understanding of cybercrime markets generally. More information is also needed to document the extent to which ideological actors recognize the value of cyberattacks, and the number of attacks that have been performed but failed for some reason. Such information is essential to document the role of internally developed attacks compared to those enabled by a third party or facilitator. In addition, this could enable our understanding of whether ideological cyberattacks can be thought of through traditional organizational models of terror and extremist violence (i.e. loners versus lone wolves).

Additional data is also needed to understand the radicalization process of cyberattackers, and any commonalities to that of real world violent actors. It is unclear if attackers developed their capacity as hackers first and then came to accept an ideological agenda later, or if they always had ideological beliefs and developed technological skills to act on those ideas. Such research will require the use of novel data collection methods, particularly qualitative interviews with ideologically leaning hackers and extremist group members to develop a robust sample of actors (Holt et al., 2017; Jordan & Taylor, 2003; Weimann, 2011). The insights that may be gleaned could be essential to improve our understanding of the nature of terrorism and extremist threats on and offline. This information could also be used to develop crime scripts and knowledge to form evidence-based defensive strategies to prevent future cyberattacks from occurring (Holt & Bossler, 2016).

References

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for cybercrime tools and stolen data: Hackers' bazaar. Rand Corporation.

Andress, J., & Winterfeld, S. (2013). *Cyber warfare: Techniques, tactics and tools for security practitioners*. Elsevier.

Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace.* New York: ABC-CLIO.

Britz, M. T. (2015). Terrorism and technology: Operationalizing cyberterrorism and identifying concepts. In T. J. Holt (ed.), *Crime on-line: Correlates, causes, and context,* (pp. 193-220). Raleigh, NC: Carolina Academic Press.

Denning, D. E. (2011). Cyber conflict as an emergent social phenomenon. In T. J. Holt & B. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 170-186). New York: IGI-Global.

Department of Homeland Security. (2009). *Assessment: Leftwing extremists likely to increase use of cyberattacks over the coming decade.* Washington, DC: Department of Homeland Security.

Dhanjani, N., & Rios, B. (2008). Bad sushi: Beating phishers at their own game." Presented at the Annual Blackhat Meetings, Las Vegas, Nevada.

Franklin, J., Paxson, V., Perrig, A. and Savage, S., (2007). An inquiry into the nature and causes of the wealth of Internet miscreants. *ACM Conference on Computer and Communications Security (CCS),* pp.275-288, Alexandria, VA: ACM.

Freilich, J. D., Chermak, S. M., Belli, R., Gruenewald, J., & Parkin, W. S. (2014). Introducing the United States extremis crime database (ECDB). *Terrorism and Political Violence*, *26*(2), 372-384.

Holt, T. J. (2013). Examining the Forces Shaping Cybercrime Markets Online. *Social Science Computer Review*, *31*(2), 165–177.

Holt, T. J., & Bolden, M. S. (2014). Technological Skills of White Supremacists in an Online Forum: A Qualitative Examination. *International Journal of Cyber Criminology*, *8*(2): 11-30.

Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. London: Routlede.

Holt, T. J., Freilich, J. D., & Chermak, S. M. (2017). Exploring the subculture of ideologically motivated cyber-attackers. *Journal of Contemporary Criminal Justice* 33: 212-233.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies*, *23*(1), 33-50.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and Estimating the Revenues and Profits of Participants in Stolen Data Markets. *Deviant Behavior*, *37*(4), 353-367.

Holz, T., Engelberth, M., & Freiling, F. (2009). Learning more about the underground economy: A case-study of keyloggers and dropzones." In M. Backes, & P. Ning (eds.), *Computer Security ESCORICS*, (pp. 1-18). Berlin and Heidelberg, Springer.

Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services. *Deviant Behavior*, 37: 1163-1178.

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: disruption and intervention approaches. *Global Crime*, *18*(1): 11-30.

Jordan, T., & Taylor, P. (2003). *Hacktivism and cyberwars: Rebels with a cause?* London: Routledge.

Karami, M., Park, Y., & McCoy, D. (2015, August). Stress testing the booters: Understanding and undermining the business of DDoS services. *Computer Science.* Retrieved from https://arxiv.org/pdf/1508.03410v1.pdf

Moore, T., Clayton, R., and Anderson, R. (2009). The Economics of Online Crime. *Journal of Economic Perspectives,* 23: 3-20.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An Analysis of Underground Forums. *IMC'11*, 71-79.

Peretti, K. K. (2008). Data breaches: what the underground world of carding reveals. *Santa Clara Computer & High Tech. Law Journal* 25: 375-384.

van Hardeveld, G. J., Webber, C., & O'Hara, K. (2017). Deviating From the Cybercriminal Script: Exploring Tools of Anonymity (Mis) Used by Carders on Cryptomarkets. *American Behavioral Scientist*, *61*(11): 1244-1266.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. London: Polity.

Weimann, G. (2011). Cyber-fatwas and terrorism. *Studies in Conflict & Terrorism* 34: 765-781.

Chapter 6. Modelling Terrorist Technology Transfer

Rebecca Earnhardt
National Consortium for the Study of Terrorism and Responses to Terrorism
University of Maryland
rearnhar@umd.edu

Gary Ackerman
College of Emergency Preparedness, Homeland Security and Cybersecurity
University at Albany
gackerman@albany.edu

While technology transfer occurs as a routine part of commercial and scientific life, this topic remains relatively understudied in the terrorism literature. As terrorists engage in increasingly lethal and technologically sophisticated attacks, the concern surrounding terrorists acquiring cutting-edge weaponry and related technologies is accumulating. As described below, the Terrorist Technology Transfer (T3) project provided a first attempt at addressing this critical operational gap in knowledge through the exploration of extant technology transfer literature, construction of the first iteration of a T3 Model, and illustrative application of the model to an emerging technological threat. The resulting T3 Model, with its identification of common actor roles and temporal stages, could assist law enforcement, intelligence officials, and policy makers in identifying failure or choke points during the transfer process, thus facilitating identification and interdiction of T3 pathways.

Modelling and Interdicting Terrorist Technology Transfer (T3)

Part of the broad impact of technological advances is their potential to increase the asymmetric attack capabilities of terrorists and other violent non-state actors (VNSAs), who are displaying ever increasing technological sophistication and lethality. A comprehensive understanding of the processes by which terrorists and other VNSAs become aware of, pursue and ultimately acquire new technologies is thus fast becoming vital to anticipating and countering non-state threats. Cooperation and technology transfer between terrorists and other actors is far from new (see Williams, Reuter, Arthur, Cliff & Ackerman, 2011; Ackerman & Bale, 2012), and there are some well-established historical case studies that illustrate this phenomenon.[3] Yet, the rise of asymmetric (and thus dangerous) technologies requires a more holistic understanding of the dynamics involved in technology transfer, from basic patterns of technology transfer behavior to determining under what conditions such technology transfer is likely to occur and to be successful. Lacking adequate conceptualization of this threat and associated indicators will render global counterterrorism forces ill-equipped to prevent and interdict in a timely manner the transfer of the most dangerous technologies to the most dangerous actors.

To address this operationally relevant gap, the T3 project, a pilot research effort, sought to examine the reasons, mechanisms, and determinants of success that attend the transfer of technologies to

[3] One of the only systematic studies in this regard is Cragin, Chalk, Daly, & Jackson's *Sharing the Dragon's Teeth: Terrorist Groups and the Exchange of New Technologies* (2007), which is useful but presents merely a handful of case studies and provides some preliminary conclusions. Moreover, it only examines the phenomenon of technology transfer between terrorists and thus examines only one part of the terrorist technology transfer picture.

terrorists. Drawing on seed funds provided by the Department of Homeland Security, this project served to present a preliminary and theoretical consideration of the issues surrounding the transfer of technologies to terrorists, setting the stage for more rigorous and expansive analysis in later iterations. As such, the following sections will review a sample of findings derived from this effort:

- *Building the T3 Model*: the synthesis of findings from a broad literature review into a theoretical framework that captures the dynamics of the transfer process and the actors involved
- *Finding Failure Points:* applying the T3 Model prospectively to an emerging threat—the transfer of carfentanil-related production technology to terrorists—in order to illustrate the potential of a fully developed T3 Model to aid analysis and interdiction of such threats

Building the T3 Model

Kicking off the T3 model development process involved surveying the literature to define the conceptual scaffolding for the model. The topic of terrorist technology transfer has received relatively minor attention in the literature, with the exception of several key sources: *Sharing the Dragon's Teeth* by Kim Cragin et al. (2007); Brian A. Jackson's *Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption* (2005); James J. F. Forest's *Teaching Terror: Strategic and Tactical Learning in the Terrorist World* (2006); and *Aptitude for Destruction, Volume 2: Case Studies of Organizational Learning in Five Groups* (Jackson, Baker, Cragin, Parachini, Trujillo, & Chalk, 2005). The remaining literature is largely descriptive in nature, lacks in-depth analysis across cases, and fails to identify important dynamics in terrorist technology transfer. The literature review conducted for this effort expounded upon the key framing questions of the T3 project, a sample of which are presented below:

- What type(s) of transfer are discussed?
- How is the actual transfer accomplished (e.g., using existing commercial channels or illicit networks)? How long does the process take?
- What factors can facilitate the transfer?
- What obstacles can impede or jeopardize the transfer?
- Which outcome(s) have been observed? What are the determinants of these technology transfer outcomes?

Relevant concepts extracted from the literature provided a foundation for broad characterization of actor connections and interaction dynamics in this effort leading to the first iteration of the T3 Model. The T3 Model represents an initial attempt to provide a theoretical framework within which to understand the various dynamics and influencing factors surrounding the phenomenon. The roles of the actors involved and the stages in the transfer process provide the bedrock upon which the model is constructed. The model defines three primary actor roles:

- The **Transferor** (which can be a multinational corporation, a state, a transnational criminal organization, or another violent extremist organization),[4]
- One or more **Intermediaries** (not present in all cases), and
- The **Recipient** (which, according to the parameters of this project, is always a terrorist actor).

[4] Future iterations will consider individual transferors not linked to a broader organization.

Each actor type can and does take on different functions in separate instances or at different points in a single transfer process. The model captures these variations among and within transfer processes (as an example, it allows for either the Transferor, the Intermediary, or the Recipient to initiate the process).

Delineations of the different stages of the transfer process (which mostly occur in sequential order) are also represented and capture the evolution of each actor role over time. The four primary (temporal) stages are:

1. Motivation and Initiation,
2. Identification and Bargaining,
3. Actual Transfer, and
4. Successful Outcome Determination.

The model thus consists of ten discrete sections, one representing the actions of each actor type over the first three stages[5] and a single section for the outcome (since the project focuses primarily on how the transfer process pertains to the terrorist recipient). It should be noted that while the nodes within the model are conceptualized as occurring in a single, discrete flow for purposes of parsimony, in reality there can be overlap or backtracking throughout the process of technology transfer, as various elements of both the theoretical and case-specific literature suggest.

Finding Failure Points

The T3 Model can help to structure analysis and guide analysts towards asking the right questions, and to potentially provide indications of when, where, how, and why a specific technology transfer might occur. While the T3 Model is currently still in a nascent phase in its development, applying it to carfentanil-related production technology illustrates how a more fully developed version might facilitate identification of failure and interdiction points. Through the recognition and pinpointing of multiple actors along critical temporal stages of the transfer process, the T3 Model can help narrow the search to specific adversaries at particular times.

Through the illustrative application of the T3 model to carfentanil-related production technology, the utility of the model becomes apparent. Carfentanil, often described as part of the "designer drugs" (Chavan & Roy, 2015, p. 297) class, is an opioid that interacts with the central nervous system, depressing respiratory function and reducing consciousness (Fentanyl: Incapacitating agent, 2017). The chemical acquired notoriety in the national security community following the October 2002 Dubrovka Theater hostage crisis during which the Russian security forces utilized a gas containing fentanyl analogs, including carfentanil, which resulted in the deaths of 127 hostages (Fentanyl: Incapacitating agent, 2017; Pitschmann, 2014, p. 1774). Concern rapidly spread through the national security domain, and officials became alert to the possibility of aerosolizing synthetic opioids, such as carfentanil, into a chemical weapon (Robinson, 2008, p. 227). More malign adversaries like terrorists can become aware of carfentanil and its production via a variety of channels, including state use and research (Bajgar, Kassa, Fusek, Kuca, & Jun, 2015; Burch, 2016; Chemical agents of opportunity for terrorism: TICs and TIMs, 2008; Cocks & Chan, 2005; "The Moscow Theater Hostage

[5] In cases featuring no intermediary actors the associated sections will be bypassed, however, in other cases, not only might the intermediary sections represent an actor, but may characterize the impact of multiple actors fitting this role.

Crisis", 2002; Kinetz, & Dodds, 2016), medical use (as a veterinary anesthetic) ("Chemical agents of opportunity for terrorism," 2008), and general public abuse of opioids (Al-Imam, Santacroce, Roman-Urrestarazu, Chilcott, Bersani, Martinotti, & Corazza; 2016).

Of particular importance in our case, adversaries could divert the technology utilized for carfentanil production to other experimental uses such as testing and manufacturing of new chemical weapons. Actors involved in the narcotics trade—particularly involving opioids and related synthetics—attempt to remain one step ahead of law enforcement authorities by making miniscule chemical alterations to compounds related to carfentanil, fentanyl more broadly, and other related narcotics so that the priducts fall outside of the scope of current regulations (International Narcotics Control Board, 2015; Kinetz, 2016; Laanela & Merali, 2016). These efforts to remain ahead of the regulatory curve by skirting the boundary between legal and illegal production could result in an infrastructure and networks whereby the potential production of chemical weapons flies under the radar of drug enforcement and national security officials. Carfentanil is an illustrative case where the aerosolization of the chemical for quite some time evaded the attention of authorities in the United States, until the 2002 Russian use of aerosolized fentanyl analogs (Pitschmann, 2014; Fentanyl: Incapacitating agent, 2017).

In the absence of actual reported or confirmed cases of carfentanil-related technology transfer to terrorists, the model can help make some inferences about factors that might facilitate this outcome. First, the model suggests that recipients who possess territory are more likely to be successful in transfer. In addition, transfers that utilize a combination of illicit and licit transfer channels are more likely to be successful. For carfentanil-related technology transfers, terrorists may seek to order commercially available laboratory equipment while seeking more highly regulated equipment or materials, such as pill presses or precursor chemicals, via illicit routes. While resource constraints can often stymie technology transfer, if the terrorist organization or individual adversary becomes involved with drug trafficking as a new stream of funding, then it is in the process beginning the transfer of relevant technology components. Especially if it becomes involved in the production end of the drug trade, it is then a relatively short jump to access existing networks and knowledge to transfer carfentanil-related production technologies.

The model also suggests numerous potential failure points in this type of transfer. For example, during the identification phase, there can be failure to reach an agreement and failure to identify a viable transferor/recipient. Carfentanil-related production technology may be attractive to a niche market where the transferor is unable to find a customer or the recipient is unable to identify a provider. However, the potential recipient and/or transferor pool may widen with increasing public abuse of opioids, and increasing public reporting on heroin adulteration with carfentanil. Also, throughout the actual transfer process, there is the possibility that the transferor may defect at any moment, deciding against transferring the technology, or that the transferor attempts to transfer the technology but ultimately fails. As the notoriety surrounding fentanyl and fentanyl analogs grows, countermeasures may enhance interdiction rates, decreasing chances of succeeding in the transfer process.

Conclusion

The T3 project shows promise for this avenue of research having not only academic, but also operational and policy impacts. It raises the possibility of providing government stakeholders, including intelligence, law enforcement, military, and policy agencies with a variety of insights and operational tools, including:

- A framework for anticipating and evaluating at a strategic level which technologies are most likely to be successfully transferred and by which channels.
- Insights into which potential preventative measures, if any, are most likely to be successful in preventing such transfers.
- Ways to identify those terrorists most likely to take part in successful technology transfer.
- Indicators of an impending transfer that would allow authorities to disrupt/interdict/prevent a particular technology transfer before it is completed.
- Indicators of a successful transfer before the technology is used in an attack.

Among the tasks that could be undertaken in a continuation of the current effort are:

- Further developing and increasing the robustness of the T3 Model, by conducting workshops and interviews to elicit a broad range of government and non-government expert opinions on the factors that facilitate and hinder technology transfer between different terrorist contexts.
- Conducting multiple additional case studies. This would allow for the testing of more hypotheses and increasing the robustness of existing findings.
- Undertaking an extensive and detailed data collection effort to capture past technology transfer cases and code them in a manner suitable for quantitative analysis. Creating a comprehensive event-coded terrorist technology transfer (T3) dataset would allow for rigorous empirical testing of certain elements of the theoretical framework.

References

Ackerman, G., & Bale, J. M. (2012). The potential for collaboration between Islamists and Western left-wing extremists: A theoretical and empirical introduction. *Dynamics of Asymmetric Conflict*, *5*(3).

Al-Imam, A., Santacroce, R., Roman-Urrestarazu, A., Chilcott, R., Bersani, G., Martinotti, G., & Corazza, O. (2016). Captagon: Use and trade in the Middle East. *Human Psychopharmacology Clinical and Experimental*, *32*. doi: 10.1002/hup.2548

Bajgar, J., Kassa, J., Fusek, J., Kuca, K., & Jun, D. (2015). Other toxic chemicals as potential chemical warfare agents. In R. C. Gupata (Ed.), *Handbook of toxicology of chemical warfare agents* (337-345). San Diego, CA: Elsevier.

Burch, K. (2016, November 11). How Carfentanil wound up in the heroin supply. *The Fix*. Retrieved from https://www.thefix.com/how-carfentanil-wound-heroin-supply

Chavan, S., & Roy, V. (2015). Designer drugs: A review. *World Journal of Pharmacy and Pharmaceutical Sciences, 4*(8), 297-336.

Chemical agents of opportunity for terrorism: TICs and TIMs. (2008, December). *American College of Medical Toxicology, 1*.

Cocks, R. A. & Chan. J. T. S. (2005). Incapacitating agents: Weapons of mass disruption." *Hong Kong Journal of Emergency Medicine, 12*(3), 182-184. Retrieved from http://www.hkcem.com/html/publications/Journal/2005-3/P182-184.pdf

Cragin, K., Chalk, P., Daly, S. A., & Jackson, B. A. (2007). *Sharing the dragon's teeth: Terrorist groups and the exchange of new technologies.* Santa Monica, CA: Rand Corporation.

International Narcotics Control Board. (2015). Precursors and chemicals frequently used in the illicit manufacture of narcotics drugs and psychotropic substances. Retrieved from https://www.incb.org/documents/PRECURSORS/TECHNICAL_REPORTS/2015/2015-PreAR_E.pdf

Fentanyl: Incapacitating agent. (2017). In *Centers for Disease Control and Prevention*. Retrieved from https://www.cdc.gov/niosh/ershdb/emergencyresponsecard_29750022.html

Forest, J. J. F. (2006). *Teaching terror: Strategic and tactical learning in the terrorist world*. Oxford: Rowman & Littlefield Publishers, Inc.

Kinetz, E. (2016, October 8). Why would anyone use a chemical weapon to make drugs? Money. In *Associated Press*. Retrieved from https://apnews.com/db983a4cbb4e4f4391439f615a3db524/why-would-anyone-use-chemical-weapon-make-drugs-money

Kinetz, E. & Dodds, P. (2016, October 8). Governments researched Fentanyls as weapons for decades. *Associated Press*. Retrieved from https://apnews.com/7e41d2d38e2740aabe17f1ed2b67df57/governments-researched-fentanyls-weapons-decades

Jackson, B. A., Baker, J. C., Cragin, K., Parachini, J., Trujillo, H. R., & Chalk, P. (2005). *Aptitude for destruction, volume 2: Case studies of organizational learning in five groups*. Santa Monica: RAND Corporation.

Laanela, M., & Merali, F. (2016, May 24). Regulate pill press machines used to make Fentanyl tablets: Abbotsford Police. In *CBC News*. Retrieved from http://www.cbc.ca/news/canada/british-columbia/pill-press-regulations-police-fentenyl-1.3597436

Pitschmann, V. (2014). Overall view of chemical and biochemical weapons. *Toxins, 6*, 1761-1784. doi:10.3390/toxins6061761

Robinson, J. P. P. (2008).Difficulties facing the chemical weapons convention. *International Affairs, 84*(2), 223-239. Retrieved from http://www.jstor.org/stable/25144763

The Moscow Theater hostage crisis: Incapacitants and chemical warfare. (2002, November 4). *In James Martin Center for Nonproliferation Studies*. Retrieved from https://www.nonproliferation.org/the-moscow-theater-hostage-crisis-incapacitants-and-chemical-warfare/

Williams, P., Reuter, P., Arthur, R., Cliff, W., & Ackerman, G. (2011). *the potential nexus between organized criminals, terrorists and radiological and nuclear smuggling: A theoretical discussion*, START: College Park, MD.

Chapter 7. Hacking the Human Body: The Cyber-Bio Convergence

Rebecca Earnhardt
Study of Terrorism and Responses to Terrorism, University of Maryland
rearnhar@umd.edu

The Cybersecurity and Biosecurity Nexus

The increasing convergence between the fields of biosecurity and cybersecurity may result in consequences that analysts have yet considered (Hoyt & Kinsey, 2017). Biotechnology use and expertise expansion beyond practitioners have stoked concerns about a wide range of traditional biosecurity issues including shielding the outputs from advanced gene editing systems or protecting university lab data storage systems (e.g., Hoyt & Kinsey, 2017; Joung, 2013, p. 98). As biotechnology advances, including digitization and automation of systems that were once localized and only accessible to those directly involved on related research, biosecurity and cyber security fields continue to intersect. One case that illustrates the accelerated intersection between biosecurity and cybersecurity—and is an emergent issue—is the use of active implantable medical devices (IMDs) which can connect wirelessly to one or more devices external to the appliance. As Hanbat National University engineer Yeun-Ho Joung has reflected, "[f]rom the first pacemaker implant in 1958, numerous engineering and medical activities for implantable medical device development have faced challenges in materials, battery power, functionality, electrical power consumption, size shrinkage, system delivery, and wireless communication" (2013, p. 89). IMDs have become smaller, more powerful, and more integrated with its wireless surroundings (Joung, 2013).

IMD functionality enhancements are reflected in overall IMD usage in the US. According to the final 2009 worldwide survey conduct by the World Society of Arrhythmia's Project, the US had the largest number of new implantable cardiac device installations in the world totaling 225,567 (Mond & Proclemer, 2011, p. 1013). Additionally, it is estimated that 20-30% of patients with Type 1 diabetes mellitus use continuous blood glucose monitor and insulin pump systems (Grunberger et al., 2014, p. 466). The number of users, sophistication of IMD manufacturing, and increasing connectedness has sparked increased academic interest in IMD cyber security risks. Peeling away the layers of this subject reveals that research on the cyber security of IMDs is relatively alarmist, and lacks integration of key areas of biosecurity research including a behavioral understanding of the invigorated, however poorly understood, IMD hacker. What the field of biosecurity can contribute to the debate, though, is a more nuanced understanding of the adversarial aspects of the IMD threat chain through the application of qualitative, case study methodologies utilized in analyzing potential bioterrorists.

Current Understanding and Analysis of the Threat

The literature on cyber security risks of IMDs falls along two lines of argumentation: patient-focused safety measures and information-focused cyber security measures (Effiong & Oremus, 2015; Heffernan, Vetere, & Chang, 2016; Denning et al., 2008; Gupta; ; Halperin et al., 2008a; Halperin et al., 2008b; Humayed et al; Lanzola et al., 2016; Lanzola et al; Rasmussen et al., 2009; Williams & Woodward, 2015). Literature which discusses patient-focused safety measures argues that too many security measures, including limited data log accessibility, multiple log-in keys, and lack of wireless connectivity, limits the ability of the patient to monitor their healthcare and limits the ability of doctors or emergency medical technicians to quickly access this information in the case of medical emergencies (Denning et al., 2010; Lanzola et al., 2016; Lanzola et al). The primary claim is that

stricter security measures without a certain level of transparency reduces the trustworthiness of IMDs ultimately diminishing the proper use of the IMD by limiting patient access to therapy and health tracking data (Fu, 2011).

In contrast, the information-focused cyber security measures camp discusses implications of possible data exploitation and malicious use of patient data (Halperin et al., 2008a). In the 2008 landmark experiment conducted by Daniel Halperin et al., the researchers demonstrated the ease of using radio frequency to jam the electrical and data systems of an implantable cardiac device (ICD) (2008a). Other information-focused security literature, and news stories alike, have focused on the potential for a malicious actor to hack into medical devices and virtually assassinate an individual by turning the IMD on or off. Other news articles claim that IMD cyber security vulnerabilities provide routes to commit insurance fraud by intentionally altering the functionality of a personal IMD, claiming that the IMD was defective beforehand (Finkle, 2014; Government Accountability Office, 2012; Humayed et al Cyber-physical systems; Reel & Robertson, 2015). The security camp often emphasizes the large number of security gaps while describing hypothetical scenarios to advocate for stricter, security-focused regulation on medical device manufacturers (Gupta; Williams et al, 2016, p. 1-6; Williams & Woodward, 2015).

However, the safety camp and the security camp fail to address a major core concern of IMD safety and security—the demand side of the IMD cyber security risk factor equation, or the behavioral factors that may induce a malicious actor to target an IMD. The safety camp assumes that IMD systems work best under the condition of absolute transparency, providing the patient with full control without taking into account the potential for hacking. The security camp makes the unsubstantiated assumption that the wide availability of IMDs and the related cyber systems harbor valuable and readily exploitable information making IMDs attractive to a malicious actor. Technology adoption and adversary decision making literature covers in depth the topics of technology use and innovative capacity of malicious actors, but the safety and security camps fail to make this connection between the two streams of literature, resulting in overestimated claims that IMDs are a reasonably attractive target for malicious actors (Cragin, Chalk, Daly, & Jackson, 2007; Flank, 1993; Jackson, 2001, p. 183-213).

Calibrating Our Perception of the Threat

Despite the alarmist tone, cyber security analysts' and engineers' concerns regarding IMD hacking are warranted as some recent security incidents indicate. A statement issued by the Food and Drug Administration's (FDA) Division of Industry and Consumer Education (DICE) in January 2017 concerning the discovery of serious cyber security vulnerabilities in the St. Jude Medical implantable cardiac defibrillator (ICD) device and the Merlin@home transmitter reflected the continued cyber security issues faced by the producers, consumers, and providers of IMDs (DICE, 2017; Nayak, 2016). As demonstrated experimentally, individuals can alter IMDs in catastrophic ways including preventing the device from monitoring a patient's vital signs, insertion of malignant code into the device software, or intentional activation or deactivation (Wellington, 2013). Although IMDs are used largely due to necessity and/or convenience for the patient, the engineering literature claims that these cyber vulnerabilities may increase incidences of IMD hacking despite the lack of recorded, verifiable incidences of hacking (Michael et al., 2010; Soroush, Arney, & Goldman, 2016; Thierer, 2016).

Notwithstanding the absence of incident records, hacking, which is the unauthorized intrusion into a computer system, has become a centerpiece of IMD risk assessments (Cherukuri, Venkatasubramanian, & Gupta, 2003; Denning et al., 2010; Halperin et al., 2008; Lanzola et al., 2016;

Rasmussen et al., 2009; Piwek et al., 2016; Williams & Woodward, 2015). Many authors posit, without any substantiation, that it is simply a matter of time and circumstance before an IMD hacker takes action against an unsuspecting patient (Burleson & Carrara, 2014; Denning et al., 2010; Government Accountability Office, 2012; Halperin et al., 2008a; Halperin et al., 2008b; Kotz et al., 2016; Kramer et al., 2012; Lanzola et al., ; Paul, Kohno, & Klonoff, 2011; "Vagus Nerve Stimulations (VNS) AspireSR®", 2017). What these analyses severely lack is the behavioral, motivational side of the alleged lurking adversary. A more comprehensive understanding of the IMD hacker's motivations could illuminate what cyber protections may be necessary to satisfy cyber security of an IMD while avoiding impeding patient or physician access to the device. The field of biosecurity can fill in this gap through applying the methodologies from analytical work focused on bioterrorists by placing the threat of IMD hacking on a supply versus demand scale.

Currently, the literature covering IMD hacking adopts a supply-side approach to analyzing the threat. The supply-side argues that the existence of the technology to hack automatically translates to adversary capability and motivation, while not accounting for decision-making aspects on the part of the adversary, which could influence their desire to pursue IMD hacking (Ouagrham-Gormley, 2014). The supply-side, technology-focused literature on IMD cyber security makes several unsupported assumptions that inevitably inflate the perceived cyber security risks (Ouagrham-Gormley, 2013, p. 473). Supported by extensive discussions and debates about the use of unconventional weaponry by violent non-state adversaries, science and technology studies scholars have conducted empirical research demonstrating that assessments about emerging technologies inflated risks and have not reflected reality (Flank, 1993; MacKenzie & Spinardi, 1995; Ouagrham-Gormley & Vogel, 2010). These authors directly counter supply-side assumptions which equate possession with ease of use and ease of output by stressing the multiple political, social, and knowledge-based nodes within the process that are difficult to define simply by examining the technology. The current cyber security literature describing the threats faced IMDs and its patients is marred by the same flawed assumptions (i.e., IMDs that have Wi-Fi and smart phone connectivity are at greater risk of hacking).

In contrast to the supply-side, the demand-side literature may inform and moderate the supply-side approach. The demand-side zeroes in on the micro-level, sociological, and psychological processes that underlie an adversary's decision to pursue a route of attack. This perspective attacks the supply-side narrative that emphasizes the numerous vulnerabilities of IMDs, and instead focuses on how the constellation of cyber security vulnerabilities interact with the adversary decision making process. The perspective argues, just because the adversary could, does not mean they will. The demand-side, thus, attempts to bridge the gap between the explicit and tacit knowledge involved in pursuing the hacking route while also exploring the amount of effort expended throughout the technology adoption process (Jackson, 2001).

According to adversary decision-making literature, opportunity plays a general role in development of new or changed tactics. Opportunity is only a small portion of the overall adversary technology adoption decision making. Other factors including organizational requirements and expertise required on the part of the adversary to learn and to successfully utilize the new tactic such as IMD hacking limit the role of opportunity. The literature that supports this conclusion includes articles which focus on adversaries adopting novel or new tactics, techniques, or procedures as it relates to unconventional weapons. This literature is used as a proxy for cyber-related adversary-focused literature which generally lacks extensive analyses of adversary decision making. The employment of IMD hacking can be viewed as an unconventional weapon in that it does not use visible or kinetic means of attack like guns or bombs.

Access to "push to start" IMD hacking or to a sympathetic engineer, in effect providing the opportunity, may spur an adversary to pursue IMD hacking as a new tactic. Researchers agree, though, that there are major hurdles for adversaries to overcome to pursue unconventional weapons development even in situations where there is clear opportunity for adversaries to acquire or develop unconventional weapons' capabilities (Caves & Carus, 2014). These hurdles include access to materials, technologies, experienced personnel, risk acceptance, and ability to learn (Ackerman, 2016). They maintain that while technological barriers may be lower and access may be more open, which is what currently supports the supply-side argument, adversaries are unlikely to pursue unconventional weapons due to a dearth of capabilities on their part to scale-up or incorporate the unconventional weapon into an effective strategy (Cronin; Parachini; Ellis, 2014). Furthermore, there appears to be significant disincentives for state transfer or third party provision of unconventional weapons to adversaries (Caves & Carus, 2014).

A preliminary adversary model for a potential IMD hacker may involve the following characteristics: ability to adapt and learn (Ackerman, 2016; Gupta; Halperin et al; Radcliffe), access to materials which may include specialized radio frequency-enabled devices that record IMD transmissions in codes (Halperin et al; Radcliffe), experience with setting-up radio frequency-enabled devices (Halperin et al), and knowledge of coding for the target IMD if the hacker seeks to insert malicious code (Gupta). These characteristics require detailed, contextual understanding of not only coding software and radio frequencies, but also trial-and-error problem solving. The adversary needs to be able to figure out how and why they were successful or unsuccessful to adapt and learn. This requires a certain level of perseverance and patience that not all adversaries may necessarily possess. Further research, particularly by surveying engineers and hackers who are familiar with IMDs and coding, would be useful to determine the types of tacit knowledge involved in IMD hacking.

Trajectory of the Field

A fully-fledged research project would explore the cyber security risk factors that are cited commonly as key vulnerabilities in IMD hacking, and filter these cyber security risk factors through an adversary technology adoption decision making and motivational analysis. Such a project would flip the supply-side, technology-focused argument about IMDs and the role of opportunity on its head, and instead focus on the demand-side, adversary-focused arguments, driven by qualitative case study methods utilized in biosecurity research. This type of research would directly challenge assumptions that adversaries will automatically possess the capability to hack an IMD as IMDs have become increasingly accessible and wireless-capable. The role of opportunity is only one aspect of a technology adoption and decision-making process, demonstrating that focusing only on the technology availability and associated cyber vulnerabilities as the technical literature currently does inadvertently inflates the perceived risk of IMD hacking.

References

Ackerman, G. (2016). Comparative analysis of VNSA complex engineering efforts. *Journal of Strategic Security 9*(1): 119-133.

Burleson, W. & Carrara, S. eds. (2014). Security and privacy for implantable medical devices (New York, NY: Springer New York, Retrieved from http://link.springer.com/10.1007/978-1-4614-1674-6

Caves Jr., J. P. & Carus, W. S. (2014). The future of weapons of mass destruction: Their nature and role in 2030, DTIC Document.

Cherukuri, S., Venkatasubramanian, K. K. & Gupta, S. K. S. (2003). Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in Parallel Processing Workshops (IEEE, 2003), 432–39. Retrieved from http://ieeexplore.ieee.org/abstract/document/1240399/

Cragin, K., Chalk, P., Daly, S. A., & Jackson, B. A. (2007). *Sharing the dragon's teeth: Terrorist groups and the exchange of new technologies.* Santa Monica, CA: Rand Corporation.

Cronin, A. K. (2006). Terrorist motivations for chemical and biological weapons use: Placing the threat in context. *Defense & Security Analysis,20*(4), 313-320.

Denning, T. et al. (2010). Patients, pacemakers, and implantable defibrillators: human values and security for wireless implantable medical devices," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (ACM): 917–26. Retrieved from http://dl.acm.org/citation.cfm?id=1753462;

Division of Industry and Consumer Education (DICE). (2017). Safety communications - cybersecurity vulnerabilities identified in St. Jude Medical's implantable cardiac devices and merlin@home transmitter: FDA safety communication," WebContent, Retrieved from http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm

Effiong, U. & Oremus, W. (2015, March 16). Nigerians will soon have to worry about implanted pacemaker security," Slate, Retrieved from http://www.slate.com/articles/technology/future_tense/2015/03/implanted_medical_devices_and_security_in_nigeria.html

Ellis, P. D. (2014). Lone wolf terrorism and weapons of mass destruction: an examination of capabilities and countermeasures," Terrorism and Political Violence, 26(1): 211–25. doi:10.1080/09546553.2014.849935

Finkle, J. (2014). U.S. government probes medical devices for possible cyber flaws. Reuters. Retrieved from http://www.reuters.com/article/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022

Flank, S. (1993). Exploding the black box: the historical sociology of nuclear proliferation, Security Studies 3(2): 259–94.

Fu, K. (2011). Trustworthy medical device software, Retrieved from https://spqr.eecs.umich.edu/papers/fu-trustworthy-medical-device-software-IOM11.pdf

Government Accountability Office (2012). Medical devices: FDA should expand its consideration of information security for certain types of devices, *Report to Congressional Requestors*, Washington D.C. Retrieved from http://www.gao.gov/products/GAO-12-816

Grunberger, G. et al. (2014). Consensus statement by the American Association of Clinical Endocrinologists/American College of Endocrinology Insulin Pump Management Task Force, Endocrine Practice, 20(5) (2014). doi:10.4158/EP14145.PS

Gupta, S. (2012, April). Implantable medical devices: Cyber risks and mitigation approaches. Presentation delivered at the Cybersecurity for Cyber-Physical Systems, Gaithersburg, MD.

Halperin, D. et al. (2008a). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Security and Privacy*, (IEEE, 2008), 129–42, Retrieved from http://ieeexplore.ieee.org/abstract/document/4531149/

Halperin, D. et al. (2008b). Security and privacy for implantable medical devices, *Pervasive Computing, 7*(1): 30–39. Retrieved from https://doi.org/10.1109/MPRV.2008.16

Heffernan, K. J., Vetere, F. & Chang, S. (2016). You put what, where? Hobbyist use of insertable devices, 1798–1809. doi:10.1145/2858036.2858392

Hoyt, K. & Kinsey, M. J. (2017). What Biosecurity and Cybersecurity Research Have in Common, Slate, Retrieved from http://www.slate.com/articles/technology/future_tense/2017/03/what_biosecurity_and_cybersecurity_research_have_in_common.html

Humayed, A., Lin, J., Li, F., & Loo, B. (2017, December). Cyber-physical systems security–A survey. *IEEE Internet of Things Journal,4*(6): 1802-1831.

Jackson, B. A. (2001). Technology acquisition by terrorist groups: threat assessment informed by lessons from private sector technology adoption, Studies in Conflict & Terrorism 24(3): 183–213. doi:10.1080/10576100151130270

Joung, Y. (2013). Development of implantable medical devices: From an engineering perspective, International Neurourology Journal, 17(3) Retrieved from https://doi.org/10.5213/inj.2013.17.3.98

Kotz, D. et al. (2012). Privacy and security in mobile health: A research agenda, *Computer, 49*(6): 22–30

Kramer, D. B. et al. (2012). Security and privacy qualities of medical devices: an analysis of fda postmarket surveillance," ed. Brad Spellberg, *PLoS ONE, 7*(7): e40200. Retrieved from https://doi.org/10.1371/journal.pone.0040200

Lanzola, G. et al. (2016). Remote blood glucose monitoring in mHealth scenarios: A review, *Sensors 16*(12): 1–17. Retrieved from https://doi.org/10.3390/s16121983

Lanzola et al., "Going Mobile with a Multiaccess Service for the Management of Diabetic Patients"

MacKenzie, D. & Spinardi, G. (1995). Tacit knowledge, weapons design, and the uninvention of nuclear weapons, *American Journal of Sociology*, 101(1): 44–99.

Michael, K. et al., (2010). Planetary-scale RFID services in an age of uberveillance, *Proceedings of the IEEE, 98*(9): 1663–71. Retrieved from https://doi.org/10.1109/JPROC.2010.2050850

Mond, H. G. & Proclemer, A. (2011). The 11th world survey of cardiac pacing and implantable cardioverter-defibrillators: Calendar Year 2009-A World Society of Arrhythmia's Project, Pacing and Clinical Electrophysiology, 34(8). doi:10.1111/j.1540-8159.2011.03150.x

Nayak, H. (2016, August 25). MW Is Short St. Jude Medical (STJ:US), Short Position (Muddy Waters Research, LLC, Retrieved from http://www.muddywatersresearch.com/research/stj/mw-is-short-stj/

Ouagrham-Gormley, S. B. (2013). Dissuading biological weapons proliferation, *Contemporary Security Policy, 34(*3). doi:10.1080/13523260.2013.842294.

Ouagrham-Gormley, S. B. (2016). *Barriers to bioweapons: The challenges of expertise and organization for weapons development*. London: Cornell University Press.

Ouagrham-Gormley, S. B. & Vogel, K. M. (2010). *The social context shaping bioweapons (non)proliferation, biosecurity and bioterrorism: Biodefense strategy, practice, and science* 8(1): 9–24. doi:10.1089/bsp.2009.0054

Parachini, J. (2003). Putting WMD Terrorism into Perspective, *The Washington Quarterly*, 26(4):37-50.

Paul, N. Kohno, T. & Klonoff, D. C. (2011). A review of the security of insulin pump infusion systems, *Journal of Diabetes Science and Technology 5*(6): 1557–62.

Piwek, L. et al. (2016). The rise of consumer health wearables: Promises and barriers, *PLOS Medicine 13*(2): 1–9. https://doi.org/10.1371/journal.pmed.1001953

Radcliffe, J. (2011). Hacking medical devices for fun and insulin: Breaking the human SCADA system. Presented at Black Hat USA 2011, Las Vegas, NV.

Rasmussen, K. B. et al., (2009). Proximity-based access control for implantable medical devices, in *Proceedings of the 16th ACM Conference on Computer and Communications Security* (ACM, Chicago, IL: ACM, 2009), 410–19. Retrieved from http://dl.acm.org/citation.cfm?id=1653712

Reel, M. & Robertson, J. (2015). It's way too easy to hack the hospital, Bloomberg.com, Retrieved from http://www.bloomberg.com/features/2015-hospital-hack/

Soroush, H., Arney, D., & Goldman, J. (2016). Toward a safe and secure medical Internet of Things, *Industrial Internet Consortium Journal of Innovation*, 1–15.

Thierer, A. D. (2016). The right to try and the future of the FDA in the age of personalized medicine, Mercatus Working Paper, Mercatus Center at George Mason University, 1–23.

Vagus Nerve Stimulations (VNS) AspireSR®. Epilepsy Foundation. (2017). Retrieved from http://www.epilepsy.com/learn/treating-seizures-and-epilepsy/devices/vagus-nerve-stimulation/vagus-nerve-stimulations-vns

Wellington, K. (2013). Cyberattacks on medical devices and hospital networks: Legal gaps and regulatory solutions, *Santa Clara High Technology Law Journal*, *30*(2): 139–98.

Williams, M. et al., (2016). Future scenarios and challenges for security and privacy, in 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry, p. 1–6. Retrieved from http://ieeexplore.ieee.org/abstract/document/7740625/

Williams, P. & Woodward, A. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Medical Devices: Evidence and Research, 8*(1): 305–16, https://doi.org/10.2147/MDER.S50048

Chapter 8. Evolving Human and Machine Interdependence in Conflict: Advantages, Risks, and Conundrums

R.E. Burnett
College of International Security Affairs at National Defense University
robert.e.burnett.civ@msc.ndu.edu

In December 2017, nations met in Geneva, Switzerland to discuss the specter of autonomy and artificial intelligence (AI) in weaponry, with great attention toward banning the technology before we fully understand what it portends for actual warfare. How do we discern between legitimate fear for potential deleterious effects upon larger societies, and that which may be useful, perhaps even beneficial to operational and strategic gains from such technologies for the purposes of ultimate deterrence that may also serve the same outcome of making safe society? Nevertheless, a more pragmatic note was sounded by Paul Scharre, from the Center for a New American Security:

> There are many reasons why a ban seems unlikely. The technology that would enable autonomous weapons is already ubiquitous. A reasonably competent programmer could build a DIY killer robot in their garage. Militaries are likely to see autonomy as highly useful, as it will give them the ability to operate machines with faster-than-human reaction times and in environments that lack communications, such as undersea. The risk to innocent civilians is unclear – it is certainly possible to envision circumstances in which self-targeting weapons would be *better* at some tasks than people. And the most difficult problem of all is that autonomy advances incrementally, meaning there may be no clear bright line between the weapon systems of today and the fully autonomous weapons of the future (Scharre, 2017).

In this brief, I seek to make several introductory analytical points, which combined, call attention to some broad trends regarding the evolution of human-machine interdependence in conflict and how it yields further problems for us to resolve on our own as well as in play with our competitors.

1. First, we would do well to prepare for a range of possible futures and take advantage of the possibility that the Chinese and Russians may be overinvesting in more narrow kinds of AI futures.

Peter Schwartz[6], a well-known futurist, invented a method of future studies in his thought-provoking work, "The Art of the Long View." Schwartz, the founder of a particular method of scenario planning, came from the risk analysis business component of Royal Dutch Shell in the 1970s where he formed an alternative approach to engaging uncertain futures.

Rather than attempt to predict such futures in a linear fashion, he fashioned a new kind of "scenario-building" technique that ultimately was built upon a set of activities where the business and later a number of clients were counseled to review a collection of research data, past and present and to forecast a range of possible futures. The goal was to help prepare the client for a variety of futures, so that when the real future arrived, they would not be so surprised, they would more likely be

[6] https://books.google.com/books/about/The_Art_of_the_Long_View.html?id=4vcOAQAAMAAJ

familiar with what was occurring due to their previous future thinking work, and they would be able to engage it in a less destructive and more profitable manner. The change in focus was away from prediction on ultimate hard futures and toward soft preparation for a variety of futures. It is less about being right or wrong, and more about being prepared for the future that actually arrives. What has changed since Schwartz first began to employ his scenario exercises is the arrival of data analytics. Big data and analytics empower this approach by increasing our ability to picture potential futures to a much higher level of resolution and greater clarity. This sort of futures thinking combined with computational modeling and simulation allows us to generate more futures and more gamed futures than ever before. We can be better prepared for the one that will ultimately arrive. The United States has been better at realizing a variety of technology futures and our flexibility in thinking about them can continue to be an important strategic tool of leverage against our competitors.

2. Second, there continues to be a trend for disruption to how the human soldier will behave in conflict that results from new technologies that combine humans and machines.

Richard Parker at the U.S. Army Combined Arms Center in 2015 at a conference on Human Systems, presented the following problem with regard to soldier performance projected into the near future (2015). The main problem as we go forward is an increase in the cognitive demand on the soldier. Both the tactical environment of the soldier, and the strategic environment of the officer is becoming more complex and demanding with information overload. The DoD approach has been to invest in a variety of solutions (to include technological solutions) to mitigate the cognitive demand that rises in the soldier and officer as a result of growing complexity in tactical and strategic environments of operation and planning. In his diagram of cognitive demand on the soldier and applied mitigation techniques, we see the U.S. Army prescribing some more traditional solutions to mitigate cognitive demand in the form of training, leadership, and doctrine. This is in part, also designed to mitigate the effects of increased cognitive demand of new technologies, many that were and are supposed to enhance a soldier's cognitive awareness. In other words, even with prescribed solutions, there are compounding side effects.

Consider the application of the emerging science and technologies that we are increasingly adding to the soldier's toolbox for a more formal application of science and technology solutions to these problems. Let's call them hard solutions as opposed to the ones that are listed in Parker's diagram that are what we can refer to as soft solutions. The soft solutions have been identified as important and primary to the full development of the human soldier; yet coming online more quickly now are the harder solutions that science and technology will deliver as well in the form of greater human-machine symbiosis, life-science applications toward human biological innovations, and even machine replacement over human soldier applications. In the end, the human soldier has some pretty hard limits, according to many engineers, hence, there are those who are increasingly attracted to non-human, machine solutions. But, Parker's U.S. Army diagram and the human element, suggests that human soldiers also have some pretty important soft skillsets that can also be enhanced and may yet be replaceable by machines, and yet, we must also inquire about uniquely human limitations. How will these evolve as a result of emerging science and technology that are applied to the human soldier condition?

Present U.S. Army Doctrine states the following as an answer to this question. From Parker's analysis:

> To continue to dominate on the battlefield of the future, the Army must invest in its people as the most agile and adaptive resource. Preserving a technological edge will remain important but technology alone is insufficient to retain overmatch in the face of highly adaptive adversaries. The Army must seek to maintain and exploit a decisive

> cognitive edge over potential adversaries. Realizing that technology remains an essential enabler with tremendous potential in the long-term, today few technological solutions exist. To overcome this shortfall, only the optimized Soldier provides the promise of meeting the cognitive demands of a modern and complex battlefield. With a shrinking force structure and growing demands on the individual Soldier, it is essential for the Army to design institutions and programs that develop the very best talent and abilities in every member of the Total Army team. This holistic body of effort is defined as human performance optimization (Parker, 2015).

Even as the Army makes such a doctrinal-like statement, emphasizing the human element, more and more investment is taking place into hard science and technology solutions that are designed to go beyond human limitations and failures. Where the Army states that few technological solutions exist, it does not mean that we will not accelerate our research and development (R&D) to discover them in the future. As I suggested before, this comes in three flavors, human-machine symbiosis, machine replacement systems, and human life science enhancement.

3. Third, the international order is deteriorating and this will impact how states will or will not be motivated to alter their trajectories for the deployment and utilization of AI and robotic technologies in weaponry.

The same Army analysis document from which I source for my comments here suggests political and ethical dilemmas for our all-too human soldiers, despite their technological enhancements. Consider the following scenario, also sourced from Parker's analysis:

> Ubiquitous Global Surveillance: By 2030, the increased availability of commercially manufactured drones, portable cameras, and wireless bandwidth will make it possible to track nearly all activity in public spaces in near real time. The private use of drones, closed circuit television, and satellites will allow social media users, bloggers, and traditional media outlets to secure live feeds of any event on the globe within minutes and proliferate them immediately. The social impact of live broadcasting of tactical battlefield actions is likely to place extraordinary pressures on small unit leaders. In the future, leaders frequently will need to make highly stressful tactical decisions before a live global audience. In the past, leaders were expected to do the right thing when nobody was watching. By contrast, tomorrow's small unit leaders will be expected to do the right thing with the whole world watching. This increased scrutiny requires leaders steeped in cultural awareness, ethical decision-making, and professional judgment (Parker, 2015).

Consider that these soldiers and their commanders will also have to likely deal with simultaneous real-time information manipulation in the form of digital and cyber exploits that may transform reality and therefore public perception. We will need to have a complimentary cyber soldier unit working alongside the tactical unit to defend their information reality against our digital adversary, perhaps in real time.

Another option may be to replace human soldiers that are capable of making such complex decisions with machines that are more automated and this may not be as much of a burden as we might expect; this being due to the changes that we are experiencing in the international system today. What has been the legacy of 70 years of creating a more rules-based system of international relations and international law with the complex interdependence of mature international economic trade relations seems to be in retreat from increasing evidence of populist forces and autocratic leaders

coming to the fore. Many suggest that our international institutions may continue to be questioned and weakened with a corresponding increase in instability and a higher propensity for political conflict that increases the potential for greater amounts of violence being used to settle differences around the world. In such a world, some leaders may have greater leverage in their abilities to wield new kinds of weapons with new examples of boldness to do so. Where the U.S. Army is arguing for the human soldier to be capable of making better political decisions in combat events (something that seems paradoxical on the surface), perhaps the Russian Army may not ask the same of its soldiers whether they be human or machine; nor the Chinese, nor the Iranians, nor the North Koreans, nor, in such a slippery slope argument, may even the Americans under these purported evolving conditions where the actions of others begin to more powerfully limit our own choices. We may want to ponder this state of politics and technology and it may be to our benefit to seek to manage it toward desired, rational ends, before we allow our world to grow in this direction.

4. Fourth, the commingling of AI types, and intelligence, surveillance, and reconnaissance (ISR) and kinetic missions, will yield new types of strategic possibilities only after we realize new tactical and operational problem sets.

If we describe a crude spectrum of autonomy in drones today we can do so as follows: on the one end is where we are presently, with human pilots using remote control stick technology, this according to the Horowitz & Scharre typologies of autonomy as "human in the loop" (2015). In the middle, is another area where we are also operating today, where drones fly according to incorporated software/hardware technology and waypoint guidance systems, this typology known as "human on the loop." On the other end of the spectrum is a future point of operation that may or may not come over some range of time where artificial intelligence advances to where we witness what we might refer to as a synthetic or emergent pilot that may result in truly novel and complex flight events that are partially or completely independent of human input, this typology Horowitz and Scharre refer to as a more advanced "human out of the loop."

Let us refer back to the U.S. Army scenario of ubiquitous surveillance and apply it to what I have just described with regard to some powerful ISR technologies that presently exist. Most of you are aware of an American ISR technology of extraordinary capability that was declassified some years ago, known as the ARGUS platform (PBS, 2013). As a loitering ISR technology, previously the world's highest resolution camera with a 1.8-billion-pixel sensor, and the capability to record 1 million terabytes of visual data per day, ARGUS creates a very powerful wide area persistent stare for what, in some instances, may amount to forensics of events on demand. This technology has likely improved since previously acknowledged.

Let us apply these capabilities away from an ISR event and toward a kinetic event. Next, let us add in advancing computational modeling and speed that is improving on the fly as a result of an ARGUS-like technology being fed real-time data for improved autonomous outcomes as described by Horowitz and Scharre. Let me quote from their work on autonomy: "Consider the role of the human or machine control with regard to, for example, acquiring, tracking targets; aiming weapons, selecting targets for engagement, prioritizing targets, timing when to fire, and detonation." I mean to suggest that autonomous (especially fully autonomous) technology that we presently possess for ISR missions, if/when applied to kinetic missions, portend to create very powerful weapons systems of increasing capability in "human on the loop" and "human out of the loop" logic types of systems. This is where the bridge will be created in which the decision chain for lethal fire can move away from human input to machine decision.

As I suggest, this has implications for both tactical and strategic thought; for example, how do we deploy and utilize such weapons for tactical combat effectiveness as opposed to how might we consider new forms of deterrence schemes in their development and deployment at the strategic level? For this short presentation, I refer back to an important strategic technology thought experiment by Martin Libicki in the 1990s in the journal Orbis, his so-called "Telemetry of War" essay, which illustrates how revolutionary technology can thrust forward our strategic thinking to new and extraordinary points of view (1996).

5. Fifth, there are certain variations of interdependent human-machine outcomes that may be as problematic as those with fully autonomous weapons.

The following is from my publication in IEEE Technology and Society Magazine from March 2017:

> If we remove the fully autonomous weapon system from this scenario and replace it with a machine-enhanced human operator, other types of scenarios and conundrums present to us as analysts and evaluators of such systems. Let us assume that such a complex interdependent machine-human soldier is able to process information faster and with more precision. This may solve part of the problem resulting from a fully autonomous weapon system in that the machine-human hybrid soldier (something that I have referred to in previous publications as a "human information appliance") acquires more of the speed of the machine, however she/he retains more of the human element for chain of authority, responsibility, and civilian input. Since this is merely a thought experiment with little to no empirical research to date to inform our thinking, we cannot know how much machine and how much human will result in various kinetic events. Neither can we know how such entities will evolve over time: which characteristics, machine or human, will become dominate in various events and for what reasons. How can we impact this sort of personality evolution either through individual psychological prophylactics or through social policy? An interesting problem may result where some systems in an HIA may be inaccessible to the human, or under certain event parameters, whereas sub-systems could become super-ordained to remote operators as interpreted by U.S. code or other legal instruments in either deliberative or ad hoc situations (Burnett, 2017, p. 31).

We can sum up these brief comments and take this discussion to a slightly more difficult, but perhaps more palpable location. Let us move from the battlefield directly to any of our domestic criminal scenes. We are already witnessing these technologies being deployed in police and homeland security events. And, my earlier discussion of Dr. Parker's description of the problem with cognitive demand on the soldier and the evolution of soft and hard solutions too can be applied to domestic police personnel in place of combat soldiers. The environments are quite similar, the human and technological parameters too, are remarkably familiar, yet, the legal frameworks can be significantly different; in other words, the rules of the game make planning, execution, and human and societal outcomes potentially very different. Yet, both of the environments; the domestic police zone, and the foreign combat zone, are laboratories, if you will, where we must learn about how these technologies and their interplay with human beings will evolve to alter our societies as well as individual lives in the not too distant future. Americans are quite familiar with their enemies, and at times, innocents as collateral damage, dying at the hands of remote control platforms to include drones in combat zones abroad and even at home with a robot bomb in Texas. But, increasingly, Americans will begin to die in larger numbers by remote control platforms, drones, and robots operated by our enemies in human in the loop as well as human out of the loop systems, and we want to engage this future with our intellects ahead of time in a rational manner. Can we rationally engage our competitors in these

technologies to discuss their development, their risks, and their dangers, and can we incentivize behavior so as to manage their evolution for a better risk management outcome in our larger international society? This is the soft technology approach, that of arms control and diplomacy.

In order to think about preparing for some evolving futures with these technologies, let me end with posing some important questions that surround these weapon technologies, here I am specifically referring to weapons systems in the three versions of human in the loop, human on the loop, and human out of the loop logics. Under what conditions are we willing to accept American and allied combat deaths that result from these kinds of technologies? What sorts of technological kinetic event deaths to American and allied soldiers do we consider to be unacceptable and for what reasons? What technological combat kinetic death events do we consider to be of greatest concern in the near term and what slippery slope arguments apply to them that could cause us to raise our efforts to engage the Russians and the Chinese with regard to controlling the development of these technologies? Consider this potential hybrid problem where technology accelerates lethality and complicates forensics with regard to our ability to know truth and reality. One important distinction at present in the development of autonomous weapon systems is the one in which United States military authorities have stated as policy that decisions on the use of lethal force, even in AI and/or robotic systems will *always* be decisions made by humans (Garamone, n.d.). This appears to be distinct from our Russian counterparts so far in that no similar assurance has been made by their authorities combined with their ongoing technological developments in autonomous weapons (Vilmer, 2016). One potential scenario that we should consider is a future conflict where Russians employ autonomous weapons that utilize AI lethal decision-making and combine it with their now demonstrated capability to simultaneously employ social media tools and other digital tools to alter, confound, and manipulate facts toward an engineered version of events, thereby helping them to utilize the kinetic AI weapon in a more effective manner. How will the US and the West respond? If we are to use our present response to their social media tools so far, we must be concerned about such a scenario that is combined with such kinetic force. Deterrence of these kinds of weapons and these kinds of events must also be re-evaluated given recent events and trends (Chow, 2018).

Last, a few more questions arise that must also be investigate with regard to the development of these technologies and our policies designed to manage them in both foreign and domestic arenas: what are the probabilities that developments in these technologies in the military sector will accelerate the so-called problem of the weaponization of domestic police forces in the United States and other countries? Importantly, many, if not most of these trending weapon platforms research programs, to include machine and even life-science agendas, are information types of weapons, in terms of their languages (code) and corresponding technologies. What are the implications of this for human privacy and information security with regard to many of our legal-based open societies?

While there are now growing domestic and international forums to investigate these policy conundrums, their potential for real-life consequences are growing more rapidly as are they are also impacting the national security planning and outcomes of the United States. Our policy capabilities in this area are insufficient at this time to advance our knowledge and policy capabilities to a competitive strategic position in either of these dimensions. More investment is needed in a professional and intellectual capacity to advance American national security interests in human-machine evolution with regard to AI and autonomy policy and it is an urgent matter.

References

Burnett, R. E. (2017, March). Brain implants and memory. *IEEE Technology and Society Magazine*. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7879423

Chow, E. K. (2018, April 7). The Marine Corps is taking cyber warfare to the front lines. *The National Interest.* Retrieved from https://nationalinterest.org/blog/the-buzz/the-marine-corps-taking-cyber-warfare-the-front-lines-25233

Garamone, J. (n.d.). Vice Chairman: Military, nation, need dialogue about new technologies. Retrieved from http://www.jcs.mil/Media/News/News-Display/Article/645569/vice-chairman-military-nation-need-dialogue-about-new-technologies/

Horowitz, M. & Scharre, P. (2015, February 13). An introduction to autonomy in weapons systems," Working Paper, Center for a New American Security, Washington, DC, p. 8-15. Retrieved from https://www.cnas.org/publications/reports/an-introduction-to-autonomy-in-weapon-systems

Libicki, M. C. (1996, April 1). The emerging primacy of information. *Orbis, 40*(2), 261-274.

Parker, R. (2015). The human dimension in the 21st century. Retrieved from https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2015/human/TuesParker.pdf

PBS (2013, January 1). Rise of the drones [Video file]. *NOVA*. Retrieved from http://www.pbs.org/wgbh/nova/military/rise-of-the-drones.html

Scharre, P. (2017, November 14). We're losing our chance to regulate killer robots. Retrieved from http://www.defenseone.com/ideas/2017/11/were-losing-our-chance-regulate-killer-robots/142517/

Vilmer, J. J. (2016, September). Autonomous weapon diplomacy: The Geneva debates. *Ethics & International Affairs*. Retrieved from https://www.ethicsandinternationalaffairs.org/2016/autonomous-weapon-diplomacy-eneva-debates/

Biographies

Dr. Gary Ackerman

Dr. Gary Ackerman is an Associate Professor in the College of Homeland Security, Emergency Preparedness, and Cybersecurity of the University at Albany. He is also the Founding Director of the Unconventional Weapons and Technology Division at the National Consortium for the Study of Terrorism and Responses to Terrorism (START), to which he remains a Senior Advisor. Previous positions have included being the Research Director and Special Projects Director at START and before that the Director of the Weapons of Mass Destruction Terrorism Research Program at the Center for Nonproliferation Studies in Monterey, California. His research encompasses various areas relating to terrorism and counterterrorism, including terrorist motivations and capabilities for using chemical, biological, radiological, and nuclear (CBRN) weapons, terrorist innovation, extremist ideologies, threat assessment techniques, red-teaming, and the modeling and simulation of terrorist behavior. He is the co-editor of Jihadists and Weapons of Mass Destruction (CRC Press, 2009), author of multiple articles on CBRN terrorism and has testified on terrorist motivations for using nuclear weapons before the Senate Committee on Homeland Security. Dr. Ackerman possesses an eclectic academic background, including past studies in the fields of mathematics, history, law, and international relations. He completed his MA in International Relations (Strategic Studies) at Yale University and his PhD in War Studies at King's College London, which dealt with the impact of emerging technologies on terrorist decisions relating to weapons adoption.

Dr. Robert E. Burnett

R.E. Burnett, Ph.D., is Interim Dean of Faculty and Academics and Professor of International Security Studies at National Defense University. He is an analyst and theoretician in the field of emerging technologies who has been a featured speaker and researcher to the National Intelligence Council's RDAWG science and technology committee. In 2018, Dr. Burnett was a plenary speaker on Artificial Intelligence to the NATO Center for Excellence at CYCON X in Tallinn, Estonia and in 2015, Dr. Burnett was invited by the Australian Department of Defence's Defence Science and Technology Organization (DST) to give the Keynote Lecture on Humans and Autonomous Systems to the Emerging Disruptive Technologies Assessment Symposium at the University of New South Wales in Sydney, Australia. His recent publications include a chapter on UAVs and ubiquitous networks in Command and Control: Tools, Systems, and New Dimensions, Lexington/Rowan Books and his work on the evolution of human-machine symbiosis for advanced situational awareness in intelligence and combat spaces was featured in two separate issues of the IEEE Technology & Society Magazine and Homeland Security Review. He has a forthcoming publication on the legacy of the Eisenhower "military-industrial complex" speech that will appear in the French Language in Politique Americaine in 2019. Also, in 2019, he has a contributing chapter on human-machine symbiosis in conflict and war that will be published in the SMA/CENTCOM/DHS series on the Third Offset.

Dr. Burnett has conducted research and analysis for the National Intelligence Council, the Institute for Defense Analyses, the Joint Military Intelligence College, and the Homeland Security and National Defense Education Consortium. He has also been an active defense community expert in the UAV policy community through the IEEE society in the United States and Australia. Dr. Burnett has previously been professor at Virginia Military Institute (2005-2013), where he was also Director of the Science and National Security Program in Washington, DC. He was also Director of the VMI-National Defense University of Hungary International Exchange Seminar in Budapest, in which he has taught for the last seven summers. In 2003, at VMI, he held the Moody-Northen Endowed Chair in Economics and was also the 2007 & 2009 winner of the Hinman Award for Excellence in Research. From 2000 to 2005, Dr. Burnett was Associate Professor of Integrated Science & Technology at James Madison University, where he was awarded the Most Captivating Lecturer Award in 2005. From 1993 to 2000 he was Assistant Director and Assistant Professor of the Patterson School of Diplomacy & International Commerce. He holds a Ph.D. in Political Science (Outside Field -Philosophy) from the University of Missouri and an M.A. in International Affairs from the Elliot School of International Affairs at The George Washington University.

Dr. Matthew Clark

Matthew Clark, Ph.D. serves as the Senior Advisor in the Office of Innovation & Collaboration. Prior to this assignment, Dr. Clark was Director of the DHS Science and Technology Office of University Programs. For over 12 years, Clark was responsible for developing, managing, integrating, and delivering the results from a $50-million annual research and education program, which includes the DHS Centers of Excellence, the Scholars and Fellows program, and the Minority Serving Institutions program. Prior to joining DHS, Clark spent 11 years as an economist with the U.S. Environmental Protection Agency (EPA). He established and managed an Economics and Decision Sciences grant program that generated some of the most significant and widely used research results ever supported by EPA. He spearheaded an EPA-wide effort to establish measures of program benefits and cost effectiveness across all agency programs. Clark also managed the quality control and release of all regulatory economics products for EPA's Office of Water and was an industry economist in EPA's Office of Science and Technology. Prior to his time at EPA, Clark was an energy and environmental economics consultant for public and private clients, an economist and budget planner for the Washington State Department of Ecology, and a land use and environmental planner for the two largest counties in Washington State. He is the author of over 50 papers, reports, and regulatory and policy analyses. He received his Ph.D. from the University of Washington, his master's degree from Washington State University, and his bachelor's degree from the University of Massachusetts. Clark was also a Peace Corps volunteer in Guatemala in the mid-1970s.

Mr. Bennett Clifford

Bennett Clifford is a Research Fellow at the George Washington University Program on Extremism. He studies violent extremist movements and organizations in the Caucasus, Central Asia, and the Balkans, and supporters of extremist groups in the United States. A graduate of Wake Forest University, Bennett previously worked in the country of Georgia, where he researched Russian and Georgian-speaking militant Islamists. He is the co-author of the Program on Extremism report *The Travelers: American Jihadists in Syria and Iraq*, the most comprehensive, publicly available accounting of American jihadist foreign fighters in the Syrian and Iraqi conflicts to date. His research has been published in a number of academic and popular publications, including *the Atlantic*, *Lawfare*, and the *CTC Sentinel*. Bennett conducts research in English, Georgian, Russian, and Spanish.

Brigadier General Alexus G. Grynkewich

Brigadier General Alexus G. Grynkewich is the Deputy Director, Global Operations (J39). He serves as the Joint Staff focal point for cyber and electronic warfare operations, information operations, special technical operations, and sensitive DOD support to government agencies.

Gen. Grynkewich received his commission in 1993 after graduating from the U.S. Air Force Academy. He has served as an instructor pilot, weapons officer, and operational test pilot in the F-16 Fighting Falcon and F-22 Raptor. Gen. Grynkewich has commanded at the squadron and wing levels, and his staff assignments include duty at Air Combat Command, U.S. European Command, and the Headquarters Air Force. Gen. Grynkewich is a command pilot with more than 2,300 hours in the F-16 and F-22.

Education

1993 Bachelor of Science in Military History, U.S. Air Force Academy, Colorado
1994 Master of Arts in History, University of Georgia
1997 Squadron Officer School, Maxwell AFB, Alabama
2003 Air Command and Staff College, by correspondence
2006 Master of Arts in Homeland Security, Naval Postgraduate School
2006 Air War College, by correspondence
2010 Master of Science in Joint Campaign Planning & Strategy, Joint Advanced Warfighting School
2012 Leadership Enhancement Program, Center for Creative Leadership, Greensboro, NC
2013 Executive Space Operations Course, Nellis AFB, Nevada
2014 Capitol Hill Workshop, Alan L. Freed Associates, Washington, D.C.
2014 Enterprise Leadership Program, Kenan-Flagler Business School, University of North Carolina

Assignments

1. June 1993 – August 1994, Student, Air Force Institute of Technology Civilian Institutions Program, University of Georgia, Athens, Ga.
2. September 1994 – September 1995, Student, Undergraduate Pilot Training, Vance AFB, Okla.
3. October 1995 – August 1996, Student, F-16C Replacement Training Unit, 63d Fighter Squadron, Luke AFB, Ariz.
4. September 1996 – July 1999, F-16 Pilot, Chief of Training, 18th Fighter Squadron, Eielson AFB, Alaska
5. August 1999 – December 2001, F-16 Instructor Pilot, Flight Examiner, and Flight Commander, 421st Fighter Squadron, Hill AFB, Utah
6. January 2002 – January 2003, F-16C Instructor Pilot and Chief of Weapons, 80th Fighter Squadron, Kunsan AB, Republic of Korea
7. February 2003 – August 2005, F-16C and F-22A Operation Test and Evaluation Instructor Pilot, 422d Test and Evaluation Squadron; Chief, F-22A Standardization and Evaluation, 53d Test and Evaluation Group; Director of Operations, 59th Test and Evaluation Squadron, Nellis AFB, Nev.
8. September 2005 – December 2006, Student, Naval Postgraduate School, Monterey, Calif.
9. January 2007 – December 2007, Chief, Interoperability Branch, 5th Generation Fighter Division; Executive Officer, Directorate of Requirements (A8), Headquarters Air Combat Command, Langley AFB, Va.
10. January 2008 – June 2009, Commander, 49th Operations Support Squadron, Holloman AFB, N.M.

11. July 2009 – June 2010, Student, Joint Advanced Warfighting School, Norfolk, Va.
12. July 2010 – May 2012, Joint Operational Planner, Chief, Crisis Response Branch, and Chief, Plans Division (J35), Headquarters U.S. European Command, Stuttgart, Germany
13. June 2012 – May 2013, Vice Commander, 57th Wing, Nellis AFB, Nev.
14. May 2013 – June 2015, Commander, 53d Wing, Eglin AFB, Fla.
15. June 2015 – June 2016, Chief, Strategic Planning Integration Division, Deputy Chief of Staff for Plans and Requirements (A5/8), Headquarters Air Force, Pentagon, Washington, D.C.
16. June 2016 – June 2017, Deputy Director for Operations, Operations Team Three, J3, The Joint Staff, Pentagon, Washington, D.C.
17. June 2017 – present, Deputy Director, Global Operations (J39), J3, The Joint Staff, Pentagon, Washington, D.C.

Summary of Joint Assignments

1. July 2010 – May 2012, Joint Operational Planner, Chief, Crisis Response Branch, and Chief, Plans Division (J35), Headquarters U.S. European Command, Stuttgart, Germany, as a lieutenant colonel and colonel.
2. June 2016 – June 2017, Deputy Director for Operations, Operations Team Three, J3, The Joint Staff, Pentagon, Washington, D.C., as a brigadier general.
3. June 2017 – present, Deputy Director, Global Operations (J39), J3, The Joint Staff, Pentagon, Washington, D.C., as a brigadier general.

Flight Information
Rating: Command Pilot
Flight hours: More than 2,300
Primary aircraft flown: F-16C, F-22A
Other aircraft flown: B-1B, B-2, B-52, C-17A, E-9A, F-15D, F-15E, HH-60G, MC-12, MQ-1, MQ-9, QF-4, T-38A, U-2

Major Awards and Decorations
Defense Superior Service Medal
Legion of Merit with one oak leaf cluster
Meritorious Service Medal with five oak leaf clusters
Air Medal
Aerial Achievement Medal with four oak leaf clusters
Joint Service Commendation Medal with oak leaf cluster
Air Force Commendation Medal
Joint Service Achievement Medal
Air Force Outstanding Unit Award with Valor device and oak leaf cluster
Combat Readiness Medal with oak leaf cluster
National Defense Service Medal with bronze star
Armed Forces Expeditionary Service Medal
Global War on Terrorism Service Medal
Korean Defense Service Medal
Nuclear Deterrence Operations Service Medal

Effective Dates of Promotion

Second Lieutenant	June 2, 1993
First Lieutenant	June 2, 1995
Captain	June 2, 1997
Major	August 1, 2003
Lieutenant Colonel	September 1, 2007
Colonel	September 1, 2011
Brigadier General	May 24, 2017

Ms. Rebecca Earnhadt

Rebecca Earnhardt is a Researcher and Project Manager for the Unconventional Weapons and Technology Division at the National Consortium for the Study of Terrorism and Responses to Terrorism (START). She focuses on emerging technologies of national security concern, biological threats and biotechnology, and adversary decision making. With experience in designing and implementing red team exercises, Rebecca takes a creative and innovative approach to addressing key areas of security concern including aviation security and radiological material control. Rebecca received her M.S. in Biodefense from George Mason University, and completed a B.A. in Political Science and a B.A. in Homeland Security / Emergency Preparedness at Virginia Commonwealth University.

Mr. Glenn Fogg

Glenn Fogg is the Deputy Director for Prototyping & Experimentation within the Office of the Director, Prototyping and Concept Experimentation. His duties include overseeing program execution and providing technical and programmatic advice for prototyping and experimentation. Working with Department of Defense commands and organizations, Mr. Fogg identifies capability short falls, leverages technologies and formulates programs that can satisfy the needs, and demonstrates the new capabilities through prototyping and experimentation

In a previous assignment within the Office of the Secretary of Defense, Mr. Fogg served as the Director of the Rapid Reaction Technology Office. In this position he identified new technologies to address combating terrorism and irregular warfare operations. Under Mr. Fogg's leadership the office expanded to include oversight of emerging biometrics and forensics technologies; and, established a nontraditional approach to develop and field militarily relevant products from companies that do not typically work with the Department of Defense.

Prior to joining the Office of the Secretary of Defense, Mr. Fogg served as a Naval Flight Officer in the United States Navy. He was promoted to Captain and through the course of his Naval career, completed four tours in Patrol Squadrons. During these assignments Mr. Fogg operated P-3 aircraft that were conducting various maritime missions, including antisubmarine warfare and surveillance & reconnaissance operations. Mr. Fogg completed an operational command tour in addition to several staff assignments before retiring from the Navy in 1999.

Mr. Fogg is a native of Annapolis, Maryland. He holds a B.S. degree from the United States Naval Academy, and an M.A. degree from the Naval War College. Mr. Fogg and his wife, Linda, reside in Annapolis.

Ms. Gia Harrigan

Gia Harrigan is currently employed by the Department of Homeland Security, Science and Technology Directorate and serves as the Program Manager for DHS Centers of Excellence. Ms. Harrigan is on-site at the Naval War College, War Gaming Department and supports Homeland Security/ Homeland Defense activities. Prior to joining DHS, Ms. Harrigan served as Science Advisor at the CNO Executive Panel in Washington, DC. She began government service at the Naval Undersea Warfare Center Division, Newport, Rhode Island and has led strategic initiatives for organizational transformation, in the areas of Technology Insertion Strategies, Business War Gaming, Balanced Scorecard, and Knowledge Management.

Ms. Harrigan has completed an Advanced Studies Program in System Dynamics at the Massachusetts Institute of Technology. She has a Master of Business Administration degree from the University of Rhode Island and an undergraduate degree in Mathematics from Boston College.

Dr. Thomas J. Holt

Dr. Thomas J. Holt is a professor in the School of Criminal Justice at Michigan State University. His research focuses on cybercrime, cybeterror and the policy response to these threats. He has published over 50 articles and books on topics ranging from the social networks of computer hackers to the practices of data thieves and cybercrime markets to the attack methods employed by ideologically motivated cyberattackers. Dr. Holt's work has been funded by the Department of Homeland Security, the National Institute of Justice, the National Science Foundation, and the Australian Research Council. He is also a globally recognized expert in the study of cybercrime and cyberterror, currently serving as a fellow in the cybercrime research cluster at the Netherlands Institute for the Study of Crime and Law in Amsterdam, and as an Adjunct Professor in the School of Law at Queensland University of Technology in Brisbane, Queensland, Australia.

Dr. Gina Ligon

Dr. Gina Ligon is The Jack and Stephanie Koraleski Professor of Collaboration Science at the University of Nebraska at Omaha. She received her PhD in Industrial and Organizational Psychology with a Minor in Measurement and Statistics from the University of Oklahoma. She is a non-Resident Fellow for the George Washington University Program on Extremism, and has been part of the Department of Homeland Security (DHS) Centers of Excellence since 2010. She is the Principal Investigator and originator of the Leadership of the Extreme and Dangerous for Innovative Results (LEADIR) database.

Her research interests include profiling leaders from afar, violent ideological groups, expertise and leadership development, and collaboration management. Prior to joining UNO, she was a faculty member at Villanova University in the Department of Psychology. She also worked in St. Louis as a management consultant with the firm Psychological Associates. She has published over 50 peer-reviewed publications in the areas of leadership, innovation, and violent groups, and she is the editor to the academic journal *Dynamics of Asymmetric Conflict: Pathways toward Terrorism and Genocide*.

Mr. Michael Logan

Michael Logan is a doctoral candidate in the School of Criminology and Criminal Justice at the University of Nebraska at Omaha and a research associate at the Center for Collaboration Science. He holds a master's degree in criminal justice from Radford University and a bachelor's degree in criminology from Lynchburg College. His research interests focus on violence, violent extremism, and criminal organizations. Michael has worked on projects funded by the Department of Homeland Security (DHS), the Department of Defense (DoD), and the National Consortium of Studies of Terrorism and Responses to Terrorism (START). Michael is currently working alongside Dr. Gina Ligon on the Leadership of the Extreme and Dangerous for Innovation Results (LEADIR) dataset. Michael's research has appeared in *Perspectives on Terrorism* and *Homeland Security Affairs.*

Dr. Robert McCreight

Robert McCreight retired in 2004 after 20 years with the State Department and other federal agencies, along with 23 years of military service in U.S. Army Special Operations and intelligence work. He has worked on nuclear, chemical and biological weapons issues, treaty verification, global scientific exchanges, counter-terrorism, threat analysis and Soviet defense policy. He has authored or contributed to five books and published over 34 journal articles. His post-doctoral work has focused on political science and public administration and he continues to teach graduate school at several universities. He has also been a periodic lecturer at National Defense University and the U.S. Army War College. His current research interests involve advanced dual use technology, foreign and defense policy, intelligence analysis, strategic wargaming and issues central to homeland security and homeland defense.

Mr. Don Rassler

Don Rassler is an Assistant Professor in the Department of Social Sciences and Director of Strategic Initiatives at the Combating Terrorism Center (CTC) at the U.S. Military Academy at West Point. His research interests are focused on how terrorist groups innovate and use technology and understanding the changing dynamics of militancy in South and Central Asia. Rassler has advised a number of operational units and been interviewed by various media outlets. He is the co-author of Fountainhead of Jihad: The Haqqani Nexus, 1973-2012, a book released by Oxford University Press in 2013.

Prior to joining the CTC, Rassler worked on intelligence, defense reform, and NATO transformation projects for the Department of Defense as a Senior Consultant at Detica. He holds an M.A. in International Affairs from Columbia University's School of International and Public Affairs and a B.S. from the University of Oregon.

Ms. Mariah Yager

Ms. Mariah Yager serves as Deputy for the Strategic Multilayer Assessment (SMA) Program under the Joint Staff/J-39, DDGO. She is a Senior Research Analyst with NSI. From 2010 to 2017, Ms. Yager helped to develop a scientifically valid, replicable, and operationally trainable discourse analysis methodology. This methodology has been used to examine insurgent writings, the expression of trust and worldview, and cognitive complexity, both in the vernacular and English translations.

Ms. Yager received her Master's in Professional Communication from Purdue University of Fort Wayne and Bachelor degrees in Anthropology and Interpersonal and Group Communication, from Indiana University and Purdue University, Fort Wayne (IPFW) respectively. Ms. Yager has taught fundamental communication theory and public speaking at IPFW and previously worked in the private sector in client management and assessments for an executive coaching and consulting firm.