

7-27-2023

Microtargeting Unmasked: Safeguarding Law Enforcement, the Military, and the Nation in the Era of Personalized Threats

Greg Lindsay
g@greglindsay.org

Jason C. Brown
United States Military Academy, jason.brown@westpoint.edu


Brian David Johnson
Arizona State University, bdj.futurist@gmail.com

Christopher Owens
United States Secret Service, christopher.owens@usss.dhs.gov

Andrew Hall
Marymount University, ahall@marymount.edu

Follow this and additional works at: https://digitalcommons.usmalibrary.org/aci_rp

See next page for additional authors

 Part of the [Human Factors Psychology Commons](#), [Interpersonal and Small Group Communication Commons](#), [Mass Communication Commons](#), [Military and Veterans Studies Commons](#), [Social Control, Law, Crime, and Deviance Commons](#), [Social Influence and Political Communication Commons](#), [Social Policy Commons](#), and the [Theory, Knowledge and Science Commons](#)

Recommended Citation

Lindsay, Greg; Brown, Jason C.; Johnson, Brian David; Owens, Christopher; Hall, Andrew; and Carrott, J.H., "Microtargeting Unmasked: Safeguarding Law Enforcement, the Military, and the Nation in the Era of Personalized Threats" (2023). *ACI Technical Reports*. 51.
https://digitalcommons.usmalibrary.org/aci_rp/51

This Book is brought to you for free and open access by the Army Cyber Institute at USMA Digital Commons. It has been accepted for inclusion in ACI Technical Reports by an authorized administrator of USMA Digital Commons. For more information, please contact dcadmin@usmalibrary.org.

Authors

Greg Lindsay, Jason C. Brown, Brian David Johnson, Christopher Owens, Andrew Hall, and J.H. Carrott

MICROTARGETING UNMASKED:

Safeguarding Law Enforcement, the Military, and the Nation
in the Era of Personalized Threats



A Threatcasting Lab Report





Disclaimer

The views expressed herein are those of the authors and do not reflect the position of Arizona State University, the United States Military Academy, the Department of the Army, the United States Secret Service, or any U.S. company, educational institution, or office of the United States Government.

MICROTARGETING UNMASKED:

Safeguarding Law Enforcement, the Military, and the Nation
in the Era of Personalized Threats



Analysts:

Authors: Greg Lindsay, Jason C. Brown,
Brian David Johnson (PI), Christopher Owens,
Andrew Hall, J.H. Carrott

Corresponding authors: Jason.brown@westpoint.edu, brian.david.johnson@asu.edu

For additional Threatcasting reports, visit the Army Cyber Institute page at:
<https://cyber.army.mil/Work-Areas/Threatcasting/>

Why This Poem Is Relevant:

I selected this proverb to kickoff the Threatcasting workshop because of its simplicity and power. It captures the fleeting nature of spoken words and how many people, often incorrectly, think about the workshop's resulting data and what's associated with it. The average person usually interprets data as something ethereal, a concept that has no basis in reality and at any point, can scatter into 'thin air.'

In reality, data is concrete. It remains. It lasts. It can be associated with an individual or group for years. And most importantly, it can be used against them.

Finally, this poem is relevant because it sets the tone for participants in a Threatcasting workshop. They are compelling events that contain great conversations, but the spoken words don't have the impact they need unless they are written down, turned into future threat models, and captured for the report that follows.

- **Brian David Johnson**





**Verba volant,
scripta manent**

(Translated)

**Spoken words fly away,
written words remain**

THREATCASTING PARTICIPANTS

Annette Aranda

Michael Caswell, U.S. Secret Service

Robin Champ, U.S. Secret Service

Tim Chen

Jeremiah Cottle, U.S. Secret Service

Roosevelt T. Faulkner, IBM

Renny Gleeson, Business Innovation Group, LLC

Bob Harrison, Researcher in Homeland Security and Futures Issues

Edwin Irungu

Jeremy S. Jones, U.S. Secret Service

Kevin Lentz, The Global Disinformation Lab

Justin Liaw, USNA

Greg Lindsay, Cornell Tech

Joseph Littell, Army Cyber Institute

Meghan McGrath, IBM

Melanie Moore, U.S. Secret Service

Christopher Owens, U.S. Secret Service

Ryan Shaddick, U.S. Secret Service

John Shaffer, U.S. Secret Service

Denzel Richard Titang, United States Naval Academy

Catherine Wiafe, U.S. Secret Service

Anonymous



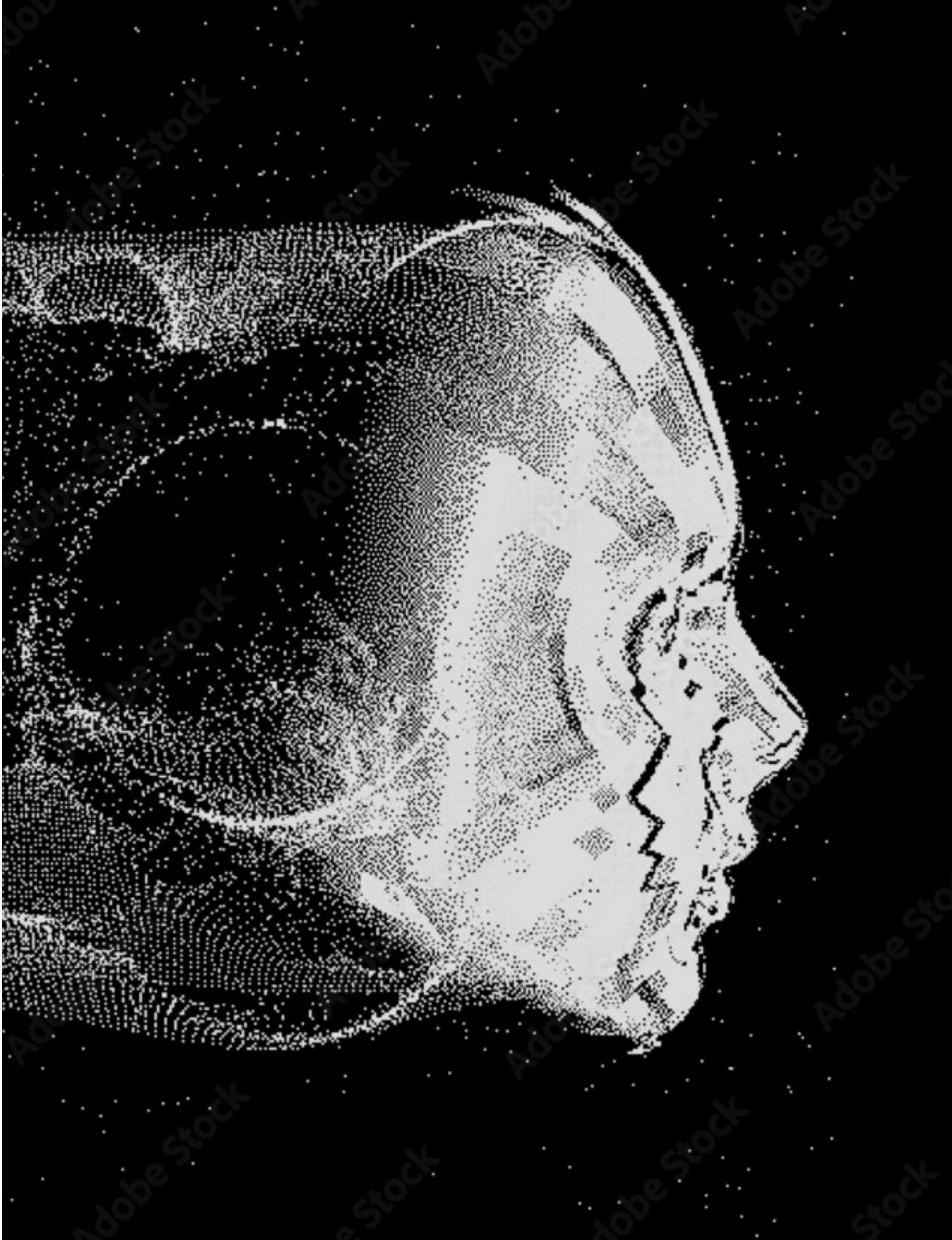
Arizona State University Threatcasting lab

The Threatcasting Lab at Arizona State University serves as the premier resource for strategic insight, teaching materials, and exceptional subject matter expertise on Threatcasting, envisioning possible threats ten years in the future. The lab provides a wide range of organizations and institutions with actionable models to better understand, identify, track, disrupt, mitigate, and recover from future potential threats. Its reports, programming, and materials will bridge gaps, and prompt information exchange and learning across the military, academia, industrial, and governmental communities.



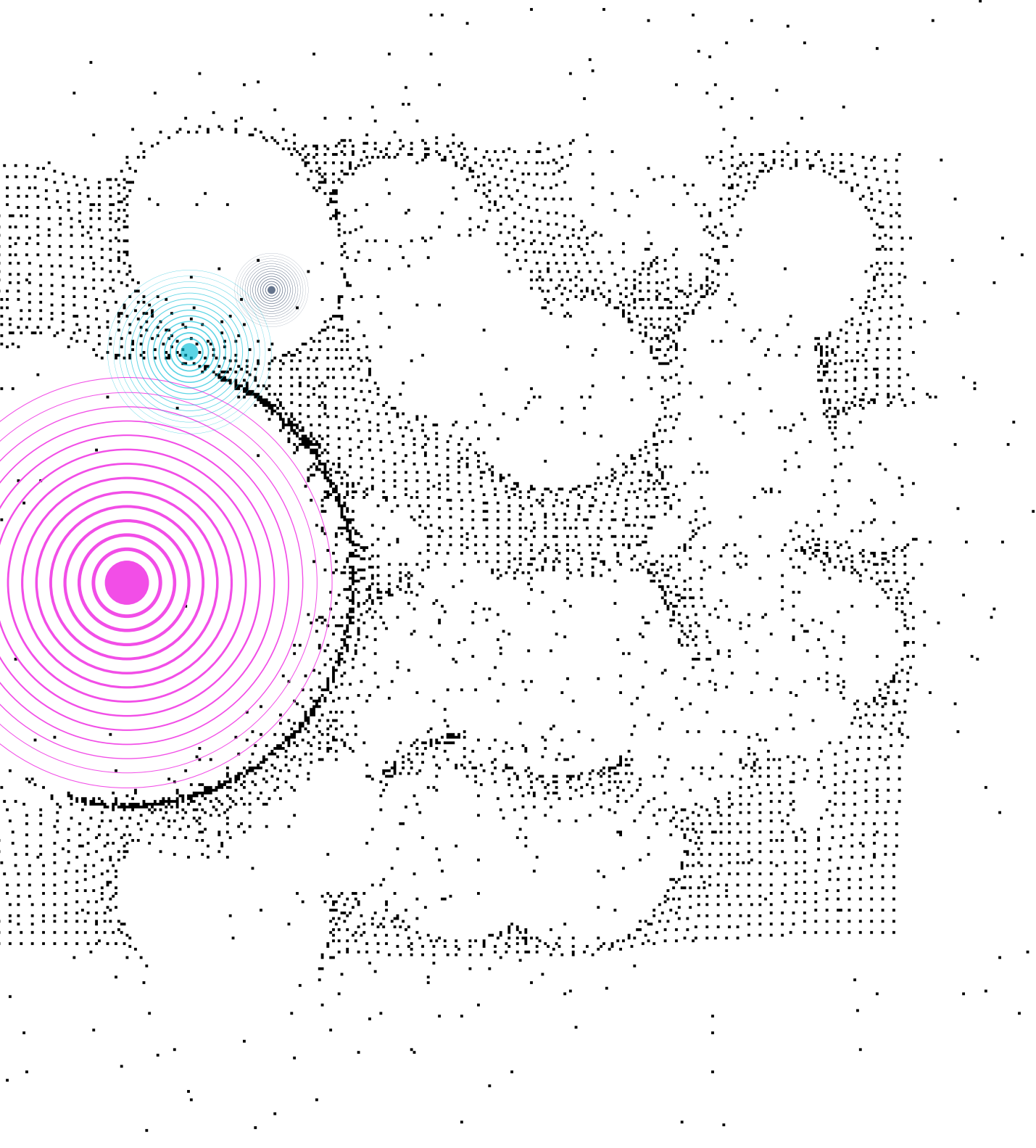
TABLE OF CONTENTS

TABLE OF CONTENTS	8
FOREWORD	10
EXECUTIVE SUMMARY	12
INTRODUCTION TO THREATCASTING	16
KEY TERMS AND ESSENTIAL CONTEXT	18
FINDINGS	30
FINDING 1: ATTACKS ON HVIS	31
FINDING 2: SOWING DECEPTION AND DISINFORMATION AMONG VULNERABLE POPULATIONS	34
FINDING 3: ATTACKS ON THE FIGHTING FORCE	36
FINDING 4: ATTACKS ON HVIS IN THE BUSINESS AND FINANCIAL COMMUNITIES	38
OUTLIERS	40
OUTLIER 1: SIMULATED INFAMY AND THE LOSS OF REPUTATIONAL SOVEREIGNTY	40
OUTLIER 2: AI CREATES TANGIBLE NEW (UN)REALITIES	43
FLAGS	44
TECHNOLOGICAL PROGRESSION	45
THE THREE SIDES OF NEXT GENERATION SECURITY	46
DEGRADING ECONOMIC AND SOCIAL CONDITIONS LEAD TO VULNERABILITIES	48
EXPANSION OF NEW INFLUENCER TYPES	49
GATES	50
DEVELOP AN ADVANCED DIGITAL DEFENSE POSTURE	50
USE HUMAN RIGHTS AS A SECURITY MEASURE	54
EXPAND EDUCATION	54
SUMMARY	56
APPENDIX A - ENGINEERING CONSENT: AN EARLY 20TH CENTURY GUIDE TO MANIPULATING THE MASSES	58
APPENDIX B - SUBJECT MATTER EXPERT INTERVIEWS	68
APPENDIX C - BIBLIOGRAPHY TO “ENGINEERING CONSENT: AN EARLY 20TH CENTURY GUIDE TO MANIPULATING THE MASSES”	94





FOREWORD



I am pleased to introduce this report jointly sponsored by the U.S. Secret Service and the U.S. Army Cyber Institute (ACI). Arizona State University's Threatcasting Lab convened experts from academia, industry, the U.S. military, and the U.S. Secret Service to explore how individuals and organizations might leverage microtargeting tactics to attack high-value individuals, or those close to them, in the U.S. military, law enforcement, other government agencies, and the public – to achieve a strategic end. Through a balanced consideration of trends and their associated implications, they developed fictional scenarios to examine how threats might evolve in an increasingly interconnected “information age” environment, and to identify possible approaches to protect against, mitigate the effects of, and recover from these attacks. The key findings – which are the views of the authors alone – are outlined in this report.

As the preeminent federal agency responsible for protecting our nation's highest elected leaders, visiting foreign heads of state, and national special security events (NSSEs), the Secret Service must continually consider novel attack scenarios against the individuals and events we protect. As a leading expert on targeted violence through the National Threat Assessment Center, the Secret Service is also committed to sharing balanced and objective research and guidance with government, law enforcement, and community partners to combat all aspects of this evolving threat, including the microtargeting of vulnerable populations.

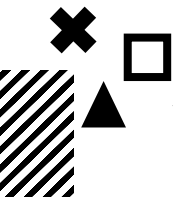
It is essential for the Secret Service – as well as other organizations – tasked with protective or defensive missions, to consider creative expert input on how the microtargeting threat is evolving. Reports such as this one – grounded in a free, open, and non-partisan conversation in an exploratory workshop setting – are instrumental for informing broader activities to identify risks and devise appropriate responses in near, mid, and long-term planning activities.

I encourage all readers to consider the vast scope of changes we have seen in recent years and imagine the broad range of tactical and operational innovations yet to come. Adopting strategic foresight methodologies and their results are essential to staying ahead of threats and protecting the nation and our leaders. I thank everyone who contributed to this effort for helping to advance the conversation on this issue.

Gregory W. Try

Chief Strategy Officer

United States Secret Service



EXECUTIVE SUMMARY

Research Questions

- How does the threat of microtargeting our forces (e.g., military, law enforcement, and/or political leaders) reveal itself over the next decade, given an increasingly interconnected “information-age” environment?
- How will this potentially affect our ability to conduct our missions to defend the nation, protect U.S. leadership, and safeguard the U.S. economy?
- What are key threats to national security due to adversaries’ ability to mine data oceans, identify, and affect individuals at scale?

Problem Area

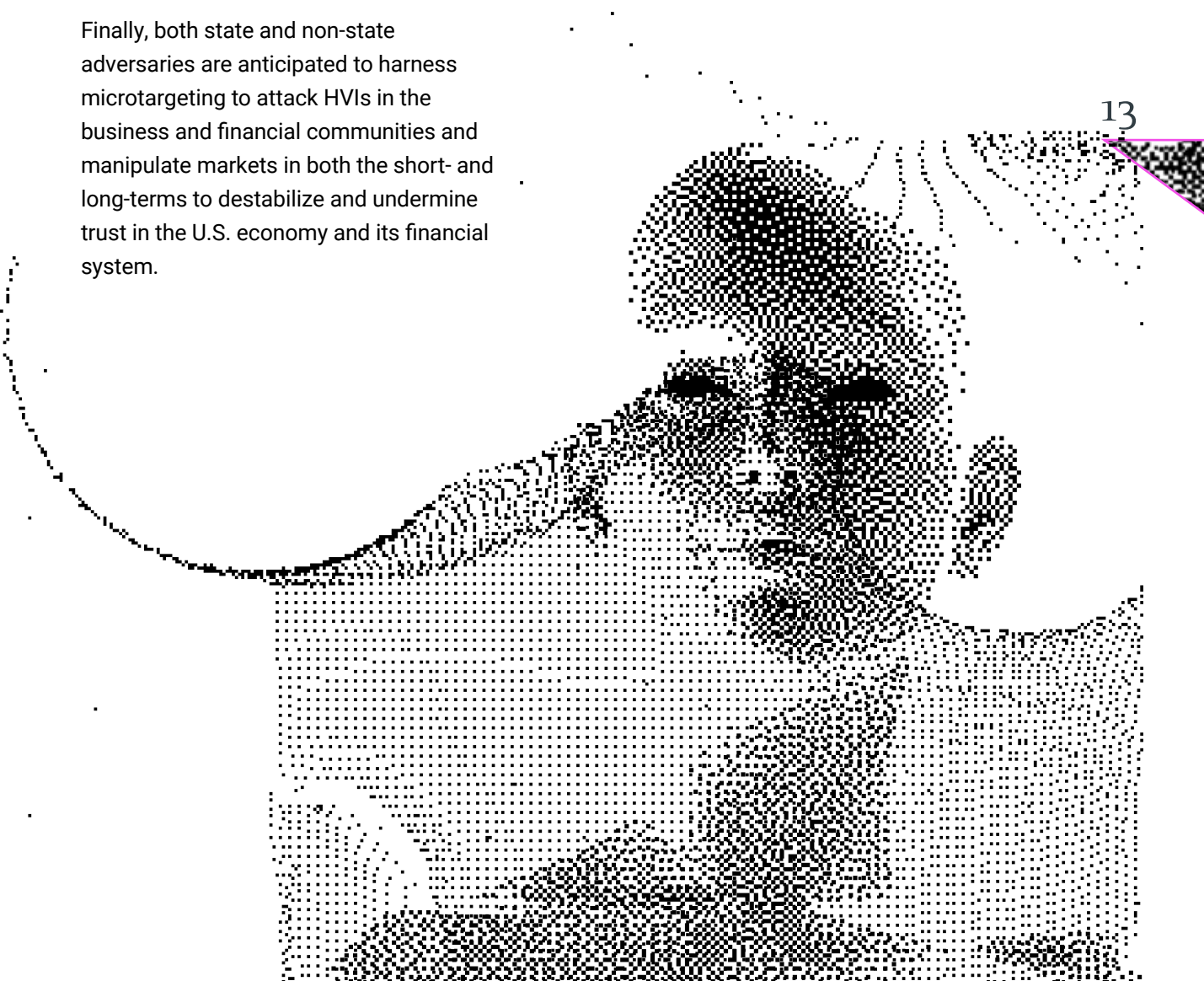
Microtargeting is the practice of collecting and analyzing personal data to create highly specific messaging for advertising, marketing, and influence campaigns. With microtargeting, the adversary’s goal is to destabilize the leadership and decision-making of federal institutions tasked with protecting the population.

This report describes how, in the coming decade, state and non-state adversaries will use microtargeting tactics to attack high-value individuals (HVIs) in military, law enforcement, and civilian leadership to stigmatize, extort, and even assassinate figures crucial to the security and stability of the United States. Adversaries will also use microtargeting tactics to manipulate and exploit individuals in proximity to HVIs when the HVI is unreachable (e.g., physical proximity, familial ties, business associates, and/or friends).

In addition to using individuals in proximity to HVIs, adversaries are also expected to target vulnerable subsets of entire populations to encourage new insider threats and exploit old grievances at scale through deception and reflexive control, a technique that gets the person to do what the manipulator wants because the person is inclined to do it. This represents an evolution of prior efforts by foreign adversaries to provoke societal division, political dysfunction, and unrest through disinformation – all in pursuit of strategic advantage.

Microtargeting attacks are also expected to be brought to bear on federal employees and military personnel to influence, radicalize, and destabilize government personnel and their loved ones, as part of a strategy to weaken the effectiveness and resolve of the fighting force. This includes both military and law enforcement organizations. These attacks are likely to employ tactics like those used against HVIs by combining aspects of both threats described above.

Finally, both state and non-state adversaries are anticipated to harness microtargeting to attack HVIs in the business and financial communities and manipulate markets in both the short- and long-terms to destabilize and undermine trust in the U.S. economy and its financial system.



Potential Responses

Microtargeting attacks require advanced resources to assist HVIs and those nearest to them recognize and respond to the attacks. Mitigation and recovery may include tools and training to recognize microtargeting attacks, capabilities for discerning and debunking disinformation in real-time, programs to recover or rehabilitate reputations, and mental health solutions to improve cognitive resilience from microtargeting attacks.

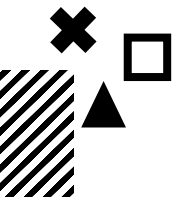
Furthermore, addressing the randomized targeting of vulnerable populations cannot be done with traditional counterintelligence or counterterrorism methods. Instead, defenders should consider responses more akin to those used for terminating the spread of a communicable disease, such as containment of the spread, careful attribution of sources, and thoughtful education of the affected population. Vulnerable populations include those who suffer from economic insecurity and/or ideological persecution; therefore, attacks against them may appear far from HVIs. Although some types of blanket targeting may appear random, they may in fact be part of a carefully planned action referred to as “stochastic terrorism.” This includes messaging and media designed to radicalize populations and inspire – overtly or covertly – acts of violence.

This report will offer possible responses to the primary research questions and additional questions that arose from our investigation, such as, “How should the federal government identify specific vulnerabilities in different populations that make them susceptible to microtargeting tactics?” Likewise, “how might national support transfer to communities and smaller populations and individuals?”

Method

This report was created from data collected over a two-day Threatcasting workshop, held at the University of Texas, Austin in November 2022. The wide range of participants who came from academia, the defense industry, commercial industry, military, and government organizations developed over 30 unique situations to envision various aspects of microtargeting threats. Threatcasting data takes the form of plausible scenarios that describe an imagined person, in a place, experiencing a version of a future microtargeting threat. These scenarios, also referred to interchangeably as models, vignettes, and science fiction prototypes, illuminate how threats to the military, federal law enforcement, and political figures might appear. Scenarios also model the conditions that need to exist before the threat is realized.



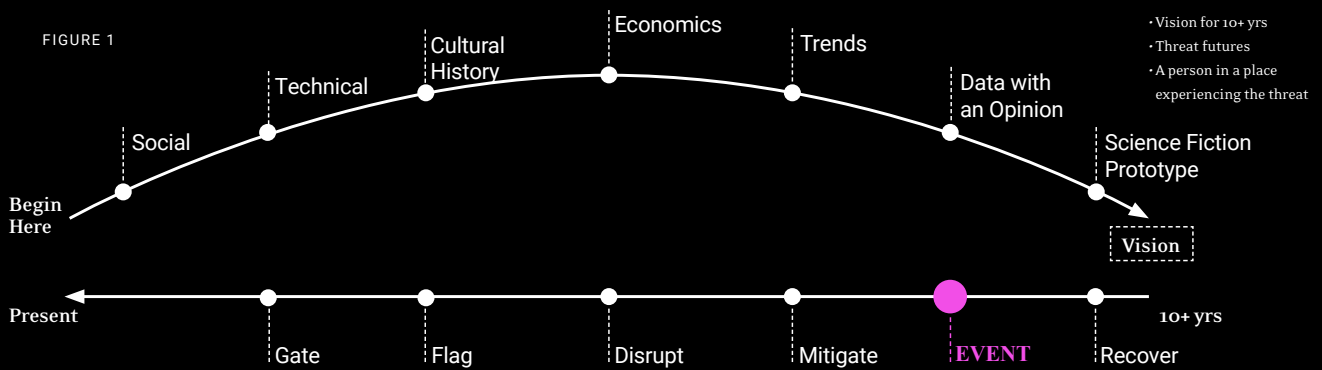


INTRODUCTION TO THREATCASTING

Threatcasting is a methodology used to help multidisciplinary groups envision future scenarios. It is a particularly powerful methodology for national security due to the ability to focus on a specific research area. This is the case with microtargeting, with emphasis on both preemptive action and post-event recovery. It is also a process that enables systematic planning against threats up to ten years in the future. Utilizing the Threatcasting methodology¹, groups explore possible future threats, how to mitigate them, and build the future they desire.

This information provides organizations and decision-makers with a framework to plan, prepare, and make decisions in complex and uncertain environments. Since the Threatcasting methodology mimics reality with science-fiction based models backed by science and Subject Matter Expert (SME) interview data, it often guards against strategic surprise. Because of this, when a crisis occurs or an opportunity presents itself, a decision-maker or a leader is better prepared. Their response is more likely to be, “We have imagined and discussed this before. We know where to start...”

Threatcasting is a continuous, multiple-step process with comprehensive inputs. These inputs range from social science, technical research, cultural history, economics,



and trends analysis. Expert interviews, sometimes called “data with an opinion,” and science fiction storytelling carefully shape inputs and trends that attempt to illustrate the research question scenarios. This dynamic set of inputs inform the exploration of potential visions of the future.

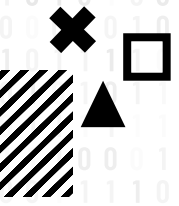
A cross-functional group of practitioners gathered for two days in November 2022 at the University of Texas at Austin to explore the future of microtargeting trends, techniques, scope and scale, as well as their implications for federal law enforcement and military forces. Participants reflected on research inputs from a diverse data set that included SME interviews (see Appendix B), synthesized the data into workbooks, and conducted three rounds of Threatcasting exercises. The purpose of the exercises was to develop effects-based models, each with a person in a place, experiencing their own version of a threat.

After the workshop concluded, the research team methodically analyzed the scenarios to categorize and aggregate indicators of how the most plausible threats could materialize during the next decade. The team also considered the potential implications for “gatekeepers” to mitigate

the threats. Gatekeepers are defined as the people, organizations, and processes that have some level of control over the resources and decisions that coincide with naturally occurring and adversary-driven events.

To that end, there are a series of indicators (“flags”) worth watching, typically outside of a gatekeeper’s control. These are paired with steps or actions (“gates”) that offer opportunities to effectively disrupt, mitigate, and recover from these potential vulnerabilities as they develop and transform into threats. The exploration of indicators and actions are grounded in the Threatcasting research questions.

The Threatcasting process enabled the participants to identify a set of plausible threats and external indicators. They then recommended actions that, if taken, are expected to mitigate the threats. While not definitive, this process provides participants, readers, and organizations a starting place to consider how future threats might manifest in certain contexts and how to address them.



KEY TERMS AND ESSENTIAL CONTEXT

In this report, we ask the primary question, “How does the threat of microtargeting our forces (e.g., military, law enforcement, and/or political leaders) reveal itself over the next decade, given an increasingly interconnected ‘information-age’ environment?” To that end, it was first necessary to address more fundamental questions, such as, “What is microtargeting?” “What is transitive data and other traits of a future information environment?” And “How is a ‘High Value Individual’ defined?”

In this section, the key terms used in this report are defined. The lexicon of microtargeting includes words and ideas with various meanings, depending on their use and context. Additional explanations of these terms also provide essential context to help frame subsequent discussions of the findings, implications, and recommended actions that follow.



1. MICROTARGETING

Microtargeting is the practice of collecting and analyzing personal data to create highly specific messaging for advertising, marketing, and influence campaigns. It leverages a broad range of data points and demographic information, such as audience interests, online behavior, and personality traits. These data points are used to identify and appeal to niche characteristics and preferences at both systemic and individual levels. This approach has proven highly effective in reaching and persuading consumers, voters, and others by leveraging personal motivations, fears, and desires.

Microtargeting emerged from political direct mail campaigns used in the 1990's, fueled by the increasing sophistication of information brokers and database marketers, such as Acxiom, which today claims to possess more than 1,500 data points per person.² The technique gained widespread attention in the early 2000s when political campaigns at various levels successfully targeted idiosyncratic voter profiles in their election efforts.³

The advent of social media added a new dimension to the practice, as billions of people were enticed to voluntarily provide deeply personal information to virtual platforms, such as Facebook. Facebook utilized this personal data to create a multi-billion-dollar advertising business, which leveraged novel methods of predicting a range of sensitive attributes, such as race, sexual orientation, and political party affiliation. This was done automatically and accurately from only a handful of self-directed "likes."⁴

Data research firm Cambridge Analytica infamously harnessed this capability by scraping the personal data of millions of Facebook users without their consent and using it to craft microtargeting influence campaigns in 2016.⁵ While the efficacy of this effort to harness information and



² Natasha Singer, "Mapping, and Sharing, the Consumer Genome," *The New York Times*, (June 16, 2012), <https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html>.

³ Luke Bunting, "The Evolution of American Microtargeting: An Examination of Modern Political Messaging," *Butler Journal of Undergraduate Research* 1 (2015).

⁴ Michal Kosinski, David Stillwell, and Thore Graepel, "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior," *Proceedings of the National Academy of Sciences* 110, no. 15 (April 9, 2013): 5802–5, <https://doi.org/10.1073/pnas.1218772110>.

⁵ Carole Cadwalladr and Emma Graham-Harrison, "How Cambridge Analytica Turned Facebook 'Likes' into a Lucrative Political Tool," *The Guardian*, (March 17, 2018), <https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm>.

influence voter behavior has been subject to intense debate, the ensuing scandal brought the issue of microtargeting to the forefront of public consciousness, which has further led to increased scrutiny and regulation. As a result, its use has expanded. State and non-state actors alike are now using these tactics.

Microtargeting remains a preferred tactic for adversarial state and non-state actors when their goals are to spread disinformation, design influence campaigns, and run financial scams. “What started as a way for businesses to connect directly with potential customers has transformed into a disinformation machine at a scale that autocratic governments of the past could only imagine,” argues Jessica Dawson, an assistant professor and research scientist at the Army Cyber Institute.⁶

For example, Facebook has been accused by journalists of embracing “a financial symbiosis with scammers, hackers, and disinformation peddlers who use its platforms to rip off and manipulate people around the world.”⁷

Looking ahead at the path to 2030 and beyond, given what has happened to date, microtargeting will likely evolve in tandem with technological advances and new cultural practices that arise from a data-saturated environment. Just as they progressed from database marketing and direct mail to social media and ubiquitous personal devices, future campaigns will

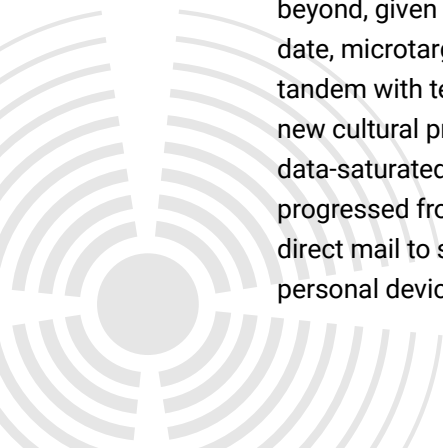
not only deploy larger volumes of more granular data, but new types of data will emerge as well, such as biometric and genetic. In addition, it is expected that there will be new tools for collection and dissemination (e.g., in “the Metaverse”), new types of connections (e.g., human-computer interfaces, brain-computer interfaces, haptics, emotional artificial intelligence), and new vectors for gaining influence, access, and control.

2. TRANSITIVE DATA

Transitive data describes a future information environment in which personal information is in multiple datasets resulting in relationships that are not just quantitatively more, but also qualitatively different. In effect, some properties will appear “entangled,” with one dataset influencing another, despite no apparent means to do so.

To describe this phenomenon, which underpins the threats posed by microtargeting, a metaphor is borrowed from mathematics. A transitive relationship is one in which properties that apply between successive numbers of a sequence must also apply between any two numbers taken in order. For instance, if A is greater than B, and B is greater than C, then A must be greater than C. — And A is considered “related” to C.

For more than a decade, attempts to understand the implications of



exponentially increasing personal data collection and storage have invariably resulted in size metaphors. “Big data” eventually led to “data lakes,” and even “data oceans” to describe datasets possessing volume, variety, and velocity too great for traditional data processing methods to control. This means many of these transitive relationships will be difficult to detect and decipher.

However, the focus on size alone excludes an even more important property, which is the emergence of unforeseen relationships across datasets and their combined ability to predict individual preferences and behavior, such as the Facebook “likes” mentioned above. Furthermore, these outcomes cannot be modeled beforehand or clearly understood due to the complexity of the connections.

Transitivity will become even more important as personal data from social media and financial transactions are increasingly combined with information that is passively processed through the Internet of Things (IoT), such as interactions with AI and virtual assistants, as well as through health and medical data collected from wearable and implantable

devices. This is in addition to use cases not yet imagined.

The nature of transitive data will favor adversaries who probe for specific microtargeting pathways versus generally understanding, mapping, and exploiting dependencies and vulnerabilities. With that said, cybersecurity organizations, such as the U.S. Cybersecurity & Infrastructure Security Agency (CISA)⁶ and the European Union Agency for Network and Information Security (ENISA)⁹ have published frameworks for reducing transitive vulnerabilities in supply chains through security by design. However, even armed with these as guides, “gatekeepers” must contend with Americans’ unshakable willingness to volunteer sensitive, personal information for marginal convenience.

3. HIGH-VALUE INDIVIDUAL

A high-value individual (HVI) is defined by the U.S. Department of the Army as a “person of interest who is identified, surveilled, tracked, influenced, or engaged.”¹⁰

⁶ Jessica Dawson, “Microtargeting as Information Warfare,” *The Cyber Defense Review* 6, no. 1 (2021): 63–79, <https://doi.org/10.31235/osf.io/5wzuq>.

⁷ Craig Silverman and Ryan Mac, “Facebook Gets Rich Off Of Ads That Rip Off Its Users,” *BuzzFeed News*, (December 10, 2020), <https://www.buzzfeednews.com/article/craigsilverman/facebook-ad-scams-revenue-china-tiktok-vietnam>.

⁸ “Securing Small and Medium-Sized Business Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks,” *Cybersecurity & Infrastructure Security Agency*, Published January 2023, https://www.cisa.gov/sites/default/files/publications/Securing-SMB-Supply-Chains_Resource-Handbook_508.pdf.

⁹ “Threat Landscape for Supply Chain Attacks,” *Report/Study*, ENISA, Published July 29, 2021, <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>.

¹⁰ Department of the Army, *Targeting*, ATP 3–60, (2015): B-1, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/atp3_60.pdf.





The Joint Chiefs of Staff, in their publication on joint targeting, relatedly describe a “high-value target” as one who “the enemy commander requires for the successful completion of the mission.”¹¹

The open-endedness of both definitions is key. For the purposes of this report, an HVI also refers to high-ranking members of the U.S. military, law enforcement, and civilian leadership. It may also refer to someone who is targeted due to their essential role in the enemy’s mission, where their value may be derived from their relative influence, accessibility, or vulnerability rather than their formal rank or position. For instance, an individual may be valuable as a proxy for targeting another HVI, in which case their value is a function of their relationship to the primary target.

Since the nature of transitive data is so complex and difficult to recognize, it will typically be difficult, if not impossible, to discern who is an HVI and why, until after an attack has occurred. Tools such as social network analysis and digital forensics may prove critical in determining potential HVIs prior to a threat being executed.

4. REPUTATION MANAGEMENT

Reputation management is the practice of monitoring, addressing, and maintaining public perception. Typically employed today by celebrities, VIPs, and high-profile organizations, it emerged in tandem with

microtargeting as a response to attacks on reputations and favorability through tactics such as search engine bombing, viral social media defamation, and faked images. In the context of this report, “reputation management” and its derivatives refer to an evolved and robust discipline more closely resembling counterintelligence than public relations.

By 2030, advanced practitioners, agent algorithms, and AI may protect HVIs from attempts to steal, capture, or doctor personal data. Other types of mitigation and recovery may include the use of forensic tools to detect potential attack vectors using transitive data as well as the combat of deepfake likenesses using novel technologies such as generative AI and assistance in social and psychological recovery following successful attacks.

Although likely to be employed on behalf of obvious HVIs at first, reputation management is poised to become an increasingly mainstream and well-resourced discipline, with practitioners in branches of the military, law enforcement, and other government agencies operating on behalf of rank-and-file members as well as VIPs. Tomorrow’s HVIs may be today’s teens who post material that future adversaries can use for leverage. This material can take the form of compromising or embarrassing selfies, comments, and/or videos.

5. INSIDER THREATS

CISA defines insider threats as “employees, contractors, and/or other trusted personnel with legitimate access to an organization’s systems and data use that access – intentionally or unintentionally – to harm its mission, resources, personnel, facilities, information, equipment, networks, or systems.”¹² They may be employees, contractors, and/or other trusted personnel with legitimate access to an organization’s systems and data. Such threats can be particularly challenging to detect and mitigate, given their default usage of standard operating procedures and security protocols. Insider threats represent a category of microtargeting subjects, unwitting proxies, and those being reflexively controlled (see definitions that follow).

The tendency for adversarial actors is to enlist insiders with diverse motivational tactics, often based on a combination of money, ideology, coercion, and ego, or “MICE.”¹³ Microtargeting might be used to recruit insider threats through any combination of MICE factors.

There are also multiple methods a bad actor will have at their disposal to compromise insider threats. They will have access to transitive data to identify insiders under financial duress, with the

ability to radicalize them through social media and generative AI. And they will be able to coerce insiders with deepfake content or leaked threats to their families and reputation to inflate the insider’s ego through various approaches. See the “Outliers” section for more on how deepfakes and generative AI support coercion.

6. STOCHASTIC TERRORISM / PROXIES






Stochastic terrorism refers to messaging and media designed to radicalize recipients and inspire acts of violence without explicitly calling for it. Drawn from mathematics, a stochastic process is one having a random probability distribution or pattern that may be analyzed statistically, but not precisely predicted. As its name implies, targets of stochastic terrorism are not predetermined, but opportunistically microtargeted with the intention that an unknown recipient will enthusiastically, and possibly unwittingly, volunteer to become an adversary’s proxy in an attack on an HVI. Because the recipient is originally unknown, the terrorist act cannot be detected prior to the incident.

Proxies, as an extension of the insider threat idea, are typically recruited from vulnerable populations who, for whatever

¹¹ Joint Staff, Joint Targeting, JP 3–60, (2013): I-9, https://irp.fas.org/doddir/dod/jp3_60.pdf.

¹² “Defining Insider Threats,” Cybersecurity & Infrastructure Security Agency, n.d., <https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats>.

¹³ Caroline D’Agati, “Want to Fight Insider Threats? Just Look for the MICE,” ClearanceJobs, Published August 2, 2019, <https://news.clearancejobs.com/2019/08/02/want-to-fight-insider-threats-just-look-for-the-mice/>.



reason, are unusually receptive to this messaging. Vulnerable populations include those who experience economic insecurity and/or ideological persecution. This form of microtargeting mirrors its original use in political campaigns to identify neglected population subsets prompting them to act. Today, this is usually done using social media platforms and other online forums to create “echo chambers” where extremist views are introduced and reinforced through propaganda and disinformation. In the future, one should expect state and non-state actors alike to employ new platforms and novel technologies with continuous influence campaigns aimed at generating a steady stream of proxies.

7. MALLEABLE ENVIRONMENTS

Malleable environments allow adversaries to influence vulnerable populations by making changes to the socio-economic, political, and cultural landscapes rather than outright manipulation of the individual. Seen as a precursor and complement to stochastic terrorism, those who seek to alter norms and discourse do so through propaganda, persuasion, and disinformation to make microtargeted individuals more susceptible to subsequent calls-to-action.

A historical example is when marketers, advertisers, and propagandists deliberately changed the environment with the contemporaneous success of the American

tobacco industry. In this situation, bad actors knowingly downplayed the harmful effects of cigarettes, while employing state-of-the-art public relations to deliberately create a culture of addiction. For more on this, see “Engineering Consent: An Early 20th Century Guide to Manipulating the Masses” in Appendix A.

8. REFLEXIVE CONTROL

Reflexive control refers to deceiving opponents into making unfavorable decisions while at the same time, convincing them that they are proper ones to make. The instigator achieves control by reaching targets with compelling disinformation and/or exploiting weaknesses in automated sensing and decision-making systems to produce desired outcomes.

Reflexive control is a term used in Russian information-psychological doctrine and generally is “a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action.”¹⁴ It can be applied to human decision-making by exploiting psycho-social inputs, such as disinformation and deception. It can also be applied to automated and machine-assisted decision-making by exploiting how the automated system receives, processes, and acts upon data.

¹⁴ Timothy L. Thomas, *Kremlin Kontrol: Russia’s Political-Military Reality* (Fort Leavenworth, KS: Foreign Military Studies Office, 2017), 176.

Reflexive control represents a third category of microtargeting subjects that is used in conjunction with willing insider threats and unwitting stochastic proxies, in that they are both simultaneously willing and unwitting participants. The adversary's goal, in this instance, is to create a tailored narrative or reality that inspires their targets to implement attacks, while the target believes they are acting in good faith.

A recent illustration of reflexive control was the 2020 SolarWinds cyberattack, which was attributed to a bad actor, presumably supported by the Russian government. In this attack, approximately 18,000 private and public sector victims downloaded a software update or "patch" in the SolarWinds suite of security software.¹⁵ For years, cybersecurity experts have emphasized the importance of updating software through regular patching. In this instance, the attacker infected the code at the source, which was the patched update itself. The narrative of safety-through-patching caused these 18,000 victims to be both willing and unwitting participants to a Russian influence operation.

9. RISK FRAMEWORK

Risk in this report refers to the probability of a specific instance of a loss of worth. This is a general definition synthesized from various risk management frameworks, including the National Institute of Standards and Technology's cybersecurity-focused risk frameworks,^{16,17} military operations security doctrine,¹⁸ and academia.¹⁹ For the purposes of this report, identifying, quantifying, and tracking future risks can be understood using a simple risk framework. This framework begins with the identification of a range of possible and potential vulnerabilities in a population, organization, country, and/or environmental or cultural condition. These vulnerabilities become threats when they are exploited by a bad actor (an individual or group) with the capability and intent to exploit the vulnerability to forward their own agenda.

¹⁵ Senate RPC, "The SolarWinds Cyberattack," Published January 29, 2021, <https://www.rpc.senate.gov/policy-papers/the-solarwinds-cyberattack>.

¹⁶ Joint Task Force, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," National Institute of Standards and Technology, (December 20, 2018), <https://doi.org/10.6028/NIST.SP.800-37r2>.

¹⁷ Joint Task Force Transformation Initiative, "Managing Information Security Risk: Organization, Mission, and Information System View," National Institute of Standards and Technology, (March 1, 2011), <https://doi.org/10.6028/NIST.SP.800-39>.

¹⁸ Department of Defense, Operations Security, Joint Publication 3-13.3, (January 4th, 2012).

¹⁹ What Is Risk? A 30,000 Foot Perspective, (Risk Bites, 2013), <https://www.youtube.com/watch?v=ijLfY06br4A>.

10. NOVEL TECHNOLOGIES

Below is a non-exhaustive list of “novel technologies” mentioned in this report that pose new threats and vulnerabilities to forces that protect the nation.

Virtualized spaces. Virtualized spaces refer to a class of increasingly immersive digital environments ranging from video games (e.g., Roblox, Minecraft, Fortnite, Call of Duty), their accompanying social media and communication platforms (e.g., Twitch, Discord), to the augmented and virtual reality “metaverse” envisioned by Meta/Facebook, Apple, and others. Together, these virtualized spaces represent a new set of attack vectors for cultivating insider threats and broadcasting stochastic terrorism. Adversaries will use them to target one’s finances or reputation and/or seek proxies through disinformation campaigns on obscure social platforms. As virtualized spaces evolve, the line between “online” and “offline” will continue to blur as wearable devices, such as audio, smart watches, and mixed-reality headsets create new opportunities for on-the-spot microtargeting.

AI virtual assistants. The overnight adoption of large language models (LLMs), such as OpenAI’s GPT-4, Google’s LaMDA, and Meta’s LLaMA heralds a new class of AI assistants for tasks. These tasks can range from ideation to coding and writing. As several high-profile incidents mentioned in this report illustrate, outputs

can be unpredictable, unverifiable, and irreproducible. Nonetheless, as their size and sophistication grow, so does their potential use for disinformation, deception, and the forming of emotional attachments that can be leveraged to produce proxies or insider threats — as, for example, OpenAI’s own red-teaming discovered.²⁰ Malicious actors might also leverage the deeply personal, individually identifiable, and permanently stored prompts LLMs used to generate outputs.

Generative AI deepfakes. Like LLMs, generative audio/visual tools, such as OpenAI’s DALL-E, Stability AI’s Stable Diffusion, and ElevenLabs’ voice cloning promise to transform the fidelity, ease, and scale of deepfaking images, audio, and video. Not only will they offer powerful new capabilities for microtargeting, including individually tailored full-scale media experiences, but they will require the creation of equally sophisticated countermeasures to detect and trace AI-based outputs. Furthermore, future variants of generative AI will be modeled on the appearance, speech, and data of trusted individuals to create “sock puppets” that will rely on pre-existing relationships with them for the purposes of deception.

Wearable and implantable devices. Today, this category includes devices, such as smartwatches, earbuds, heads-up displays (e.g., Google Glass, Microsoft HoloLens), and implanted medical devices. Future iterations will expand to include more

²⁰ OpenAI, “GPT-4 System Card,” (March 15, 2023), <https://cdn.openai.com/papers/gpt-4-system-card.pdf>

sophisticated implantable networked hardware for health, perception, and convenience. This will, in turn, create microtargeting opportunities to hack, attack, and deceive individuals in attempts to gain leverage or reflexive control.

Neurostimulation. Beyond microtargeting one's beliefs, emotions, and perceptions, the technique of neurostimulation refers to the invasive and non-invasive modulation of the nervous system, using electromagnetic means with the possibility of targeting the brain itself. Neurostimulation is foundational for neural prosthetics, such as hearing aids, artificial vision, artificial limbs, and brain-machine interfaces. In addition, as these technologies evolve, so will opportunities to capture and analyze data that is available directly from the wearer's senses and sense-making devices.

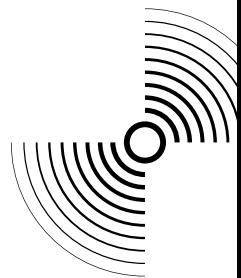
Biomedical microtargeting. Biomedical research relies on the sampling of human blood and tissue that is anonymized and transitively linked with patient data. Cyberattacks on these databases and on research databases enabled by the sale of willingly harvested DNA²¹ will allow attackers to steal and transitively add this to other types of personal data at scale. This has the capacity to reveal both a large-scale population health map, and emergent relationships between individuals' health,

financial data, and other identifying factors. Furthermore, the rapid advance of genetic editing tools, such as CRISPR, will empower practitioners to edit, follow, and/or predict changes in both individual- and population-scale DNA. This, in turn, will enable state and non-state actors to perform acts, such as design viruses or create tailored DNA that can be carried inside a common virus, such as influenza. It will also enable them to design viruses to attack specific genes that regulate the immune response as well as incapacitate or kill targets with an apparent auto-immune disease.

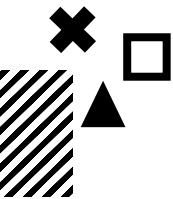
²¹ Kristen V. Brown, "23andMe Is Selling Your Data, But Not How You Think," Gizmodo, (April 14, 2017), <https://gizmodo.com/23andme-is-selling-your-data-but-not-how-you-think-1794340474>.

11. RESPONSIVE ENVIRONMENTS.

From augmented realities to responsive materials, such as smartphone-controlled paint colors,²² technology improvements will enable environments to become spaces that can respond in real time to stated and predicted human attributes and behaviors. Experiments in beam casting and beamforming—techniques to focus beams of sound and light—already allow custom, individuated audio/visual experiences in the real world, targeted to individuals standing side by side. Controlling a person’s environment may enable microtargeting via preconditioning and priming. For a deeper exploration on how changing a person’s surroundings makes them more susceptible to targeted advertisements and messaging, see “Engineering Consent: An Early 20th Century Guide to Manipulating the Masses” in Appendix A.



²² James Billington, “Colour-Changing Paint You Control with Your Smartphone Is the Future of DIY,” International Business Times UK, (October 12, 2015), <https://www.ibtimes.co.uk/chameleon-colour-changing-paint-you-control-your-smartphone-future-diy-1523669>.



FINDINGS

The findings are based on SME interviews and the workshop discussions involving representatives from the U.S. Secret Service, the U.S. Army, universities, and industry. A team analyzed the models and SME interviews for thematic patterns based on central research questions. Four main categories or “threat spaces” emerged, each focused on a difference target. Fictional scenarios are shared in call-out boxes to illustrate findings.

SCANDAL AT THE BANK

The spouse of the chairman of a major U.S. bank is driven to suicide after her parallel life as a virtual influencer is exposed. State-backed hackers steal her identity – followed shortly after by her savings, reputation, and sanity. It’s done by using spontaneously created audio, video, and social media deep fakes to bypass authentication procedures and turn public opinion against her. After months of escalating scandals, she kills herself in desperation. This in turn destroys her husband’s political career, and with it, his management of the assets entrusted to his bank. The attack is later believed to be a retaliation for U.S. economic sanctions on Israel, following their export of cyberweapons to China.

Finding 1: Attacks on HVIs

Adversaries will use microtargeting to attack figures in military, law enforcement, and civilian leadership, using transitive data and novel technologies to identify and exploit new vulnerabilities.

Microtargeting is poised to rapidly evolve into a set of tools and tactics employed by adversarial state- and non-state actors to target HVIs who are critical to the security and stability of the United States. Although the intentions and objectives of those adversaries and targets will vary, the general desired outcome of microtargeting will be to destabilize leadership and degrade the decision-making of federal institutions that are tasked with defending the country.

In addition, microtargeting may not always be aimed at HVIs per se, but rather at surrounding colleagues, direct reports, close friends, and family who might be instrumentalized through deception, coercion, and/or subversion. This expands the potential HVI population. The specific nature of the threat will depend on the target and desired outcome, ranging from kinetic attacks (e.g., towards an individual's health and well-being) to more subtle campaigns to destroy careers and reputations through planted scandals,

corruption, and/or humiliation.

This concept and practice are tied to a commonly used principle of Russian information operations, referred to as kompromat, a term short for "compromising material." In the past, the KGB used kompromat, often in the form of "sexually-embarrassing dirt on public figures" to manipulate and persuade HVIs into a particular course of action.²³ Attacks on HVIs may integrate this practice with recent technology and updated methods, which will in turn lead to new forms of kompromat.

Easier access to larger and more granular troves of sensitive personal data will likely allow microtargeting to precisely target individuals. This will not simply be a function of "big" data, but of the continued confluence of an ever-lengthening list of sources. These sources range from personal, professional, medical, and financial profiles to social media content, transaction histories, real-time location data, and traces from connected devices, etc. Collectively, this conjoined dataset-of-datasets might be more accurately referred to as transitive data, defined more by the emergent properties and relationships of their linkages as opposed to the sheer size of their sources.²⁴

²³ Jamie Seidel, "The Honey-Trap of 'Kompromat,'" News Corp Australia Network, (January 13, 2017): sec. Real Life, <https://news.com.au/lifestyle/real-life/wtf/kompromat-is-putins-bringing-the-old-kgb-honey-trap-back-to-international-politics/news-story/3a9a147bfdab20ec51d2727c810bc1b>. See also: Charles Maynes, "Russian 'Kompromat' Remains Alive and Well," VOA, (January 15, 2017), <https://www.voanews.com/a/russia-kompromat-remains-alive-and-well/3677094.html>.

²⁴ A more thorough explanation of the emerging idea of transitive data is found in the Definitions section of this report.



Inevitably, there will be entanglements of delicate information that offer determined attackers the ability to exploit individuals. Sensitive data stolen from one source might unlock access to other channels across the chain – of which the exact length and composition are unknown. This will in turn make it incredibly difficult to safeguard, allowing bad actors both access to the data and the ability to leverage linked data to harm microtargeted individuals and proxies.

New tools will also be available to bad actors, which will give them more power and access to HVIs. Likewise, these tools are expected to be used together. Examples include the use of novel technologies misused for surveillance, evasion, and deception, such as real-time deepfakes, compromised AI assistants, wearable and implantable devices, at-home gene editing kits, and more. For instance, large language models, such as OpenAI's ChatGPT have quickly spawned seemingly unstable, threatening,²⁵ and emotionally manipulative chatbots,²⁶ while televised deepfake disinformation has already been spotted emerging from Venezuela²⁷ and China.²⁸

As attacks are expected to mount on HVIs and their associates, the forces tasked with protecting them are likely to struggle with establishing a defensive perimeter around potential targets. This will also come with a realization that the properties of transitive data may make anticipating threats nearly impossible. A new practice of "reputation management" will likely emerge to combat deepfakes and other hostile tactics, but the threats may not be able to be prevented. However, they may be managed once incited. Given the targets' essential roles in defense, civil society, and the economy, the potential for escalation will require a broader effort to build more resilient systems for mitigation and recovery as well as protection.

²⁵ James Vincent, "Microsoft's Bing Is an Emotionally Manipulative Liar, and People Love It," The Verge, (February 15, 2023), <https://www.theverge.com/2023/2/15/23599072/microsoft-ai-bing-personality-conversations-spy-employees-webcams>.

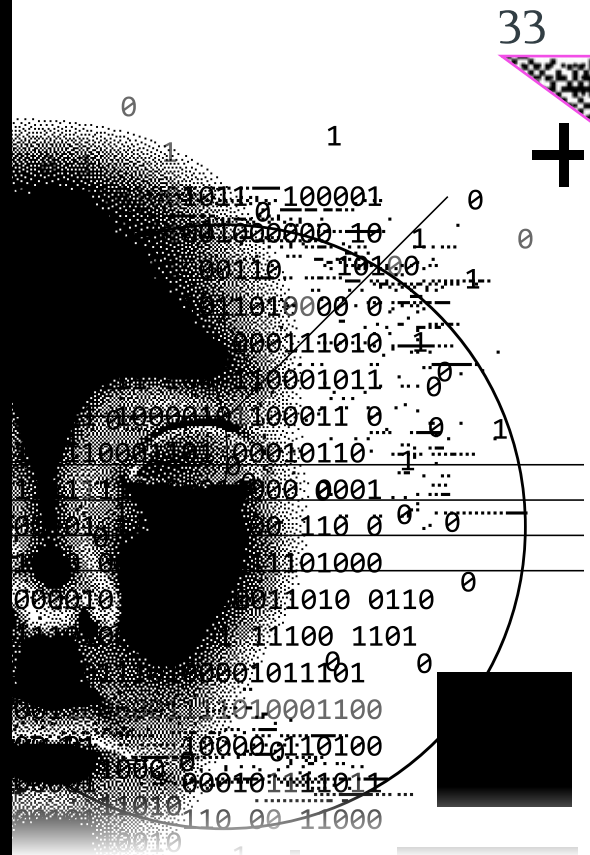
²⁶ Samantha Cole, "It's Hurting Like Hell': AI Companion Users Are In Crisis, Reporting Sudden Sexual Rejection," Vice (blog), (February 15, 2023), <https://www.vice.com/en/article/y3py9j/ai-companion-replika-erotic-roleplay-updates>.

²⁷ Florantonia Singer, "No son periodistas, son avatares: el chavismo impulsa propaganda hecha con inteligencia artificial," El País, (February 20, 2023): sec. Internacional, <https://elpais.com/internacional/2023-02-20/no-son-periodistas-son-avatares-el-chavismo-impulsa-propaganda-hecha-con-inteligencia-artificial.html>.

²⁸ Adam Satariano and Paul Mozur, "The People Onscreen Are Fake. The Disinformation Is Real.," The New York Times, (February 7, 2023):, sec. Technology, <https://www.nytimes.com/2023/02/07/technology/artificial-intelligence-training-deepfake.html>.

SILENT VIRUS, ESCALATING CRISIS

The White House physician's teenage "youthfluencer" daughter panics when her follower count crashes, unaware that her audience is almost entirely comprised of bots as part of a microtargeting scheme to reach POTUS. The adversary stealthily offers her a chance to win them back by reviewing an exclusive new "fragrance," which in reality is carrying an aerosolized virus keyed to the President's DNA. Caught in his daughter's repeated on-screen spritzing, while reviewing the fragrance, the physician unwittingly carries the virus to the Oval Office and infects the President with a mild flu. This experience causes her to withdraw to her bedroom, and malware and deepfakes are used to block information about escalating geopolitics, as other AI's play a role in escalating the situation.



Finding 2: Sowing deception and disinformation among vulnerable populations

Adversaries will continue to microtarget vulnerable subgroups to develop insider threats and proxies.

Microtargeting was invented to identify and locate increasingly small voter blocs who stood apart from their surrounding electorate and were unresponsive to mainstream norms and messaging. In the two decades since its initial use, the addition of a precarious economy, widening U.S. income inequality,²⁹ political polarization, and online echo chambers have created an environment that is extremely vulnerable to microtargeting of the disenchanting and disenfranchising. Adversaries can leverage these variables to trigger societal division in pursuit of strategic advantage.

For example, prior to the U.S. presidential election in 2016, Russia's Internet Research Agency posted disinformation on dueling Facebook groups to independently organize protests alternately opposing and defending a Houston mosque.³⁰ In another

example, later that year, high level political emails were reportedly stolen by Russian-sponsored operatives.³¹ This became the seed of a child trafficking conspiracy that would grow and morph into a well-known U.S.-based conspiracy group. In both cases, microtargeting attacks provided the spark that rapidly divided populations and spread paranoia.

A current example is the ongoing evolution of a right-wing radicalized channel designed for the Generation Z population that uses platforms, such as TikTok to indoctrinate young audiences with precisely calibrated memes and language.³² Joshua Citarella, an artist and internet culture researcher, and others persuasively argue that Generation Z is at least partly predisposed to this messaging due to, what has been described as, barely suppressed despair. As the artist and technologist James Bridle posits in his book *The New Dark Age*, contemporary conspiracy thinking functions as "a kind of folk knowing: an unconscious augury of the conditions, produced by those with a deep, even hidden, awareness of current conditions and no way to articulate them in scientifically acceptable terms."³³

²⁹ Juliana Menasce Horowitz, Ruth Igielnik, and Rakesh Kochhar, "Most Americans Say There Is Too Much Economic Inequality in the U.S., but Fewer Than Half Call It a Top Priority," Pew Research Center, (January 9, 2020), <https://www.pewresearch.org/social-trends/2020/01/09/trends-in-income-and-wealth-inequality/>.

³⁰ Martin J. Riedl et al., "Reverse-Engineering Political Protest: The Russian Internet Research Agency in the Heart of Texas," *Information, Communication & Society* 25, no. 15 (November 18, 2022): 2299–2316, <https://doi.org/10.1080/1369118X.2021.1934066>.

³¹ Lorenzo Franceschi-Bicchieri, "How Hackers Broke Into John Podesta and Colin Powell's Gmail Accounts," *Vice*, (October 20, 2016), <https://www.vice.com/en/article/mg7xjb/how-hackers-broke-into-john-podesta-and-colin-powells-gmail-accounts>.

³² Nathan Taylor Pemberton, "The Young Political Spaces of the Internet," *The New Yorker*, (March 17, 2021), <https://www.newyorker.com/culture/cultural-comment/the-young-political-spaces-of-the-internet>.

³³ James Bridle, *New Dark Age: Technology and the End of the Future* (Verso, 2018).

The result is an infinite array of subgroups susceptible to microtargeting, whether that means recruiting unwitting proxies for straightforward reasons; sowing disinformation to inspire random radicalization; or by using reflexive control to align their own objectives with the already radicalized.

Once again, novel uses of innovative technology may influence how subgroups are targeted. Bad actors are expected to use malfunctioning, compromised, and stealthily malicious AIs to create impenetrable filter bubbles tailored to individuals and groups.³⁴ They will curate content for users that only shows what the conspiratorial AIs want them to see and nothing else. Virtualized spaces, such as Twitch, Discord, and VRChat, and/or their successors will offer adversaries malleable environments in which to test messaging and recruitment techniques. The line between fantasy and reality may become nearly impossible to distinguish, as humans overuse cameras, sensors, and devices whose outputs can be altered, spoofed, or faked.

Both Facebook in 2016 and QNet in the fictional future “Rescue the Children!” are examples of malleable environments in which the goal is not to target individuals directly, but to imperceptibly alter the circumstances of their decisions. The next step is stochastic terrorism, the microtargeting of a vulnerable subset of the population in hopes that a random member or members will effectively volunteer to attack the HVIs in question.³⁵

The stochastic targeting of vulnerable groups will require a response that mimics the combatting of an epidemic more so than traditional counterintelligence or counterterrorism efforts. Because of this dynamic, it is important to address more questions, such as “Who is susceptible to simulated attacks and why?” “How should the federal government identify specific vulnerabilities in various populations?” “How might it prepare for and safeguard against them?”

³⁴ Ben Thompson, “From Bing to Sydney,” Stratechery (blog), (February 15, 2023), <https://stratechery.com/2023/from-bing-to-sydney-search-as-distraction-sentient-ai/>.

³⁵ Additional information on the concept of stochastic terrorism can be found in the “Definitions section” of this report.

RESCUE THE CHILDREN!

A former Amazon warehouse worker outfitted with neurological and ocular implants has become an avid user of "QNet," an app seemingly released by QAnon true believers who publish sensory playback of their fury for those with the proper tech. Adversaries planning an attack on an upcoming G7 Summit use the app and its trove of psychological and biological profiles to select the worker to witness their deception. After remotely triggering QNet's abilities to influence his nervous system, he observes a seemingly real, yet completely faked child abduction by agents of the city's S.W.A.T. team. He then proceeds to record, upload, and fervently share this virtual encounter as evidence of his own experience. The viral clip becomes a rallying cry for armed QNet members to converge on the summit to rescue the "children held inside." The ensuing bloodshed is impossible for anyone to deny.

Finding 3: Attacks on the fighting force

Microtargeting will be used to target military personnel and civilian federal employees in a sustained effort to weaken American defenses.

As microtargeting tools become more affordable to the average person, increase in scale, and are more capable of harnessing transitive data, the definition of an HVI are expected to expand to the forces tasked with protecting the nation and American way of life.

Attacks on soldiers, law enforcement, and supporting agencies will likely be low-level

and persistent. It is expected that they will be aimed primarily at compromising security systems and facilities, and will degrade individual and unit cohesion, while undermining public trust. Also expected are tactics like those deployed against HVIs, including corruption through financial incentives, psychological isolation, radicalization, and preying on insecurities.

These vulnerabilities have share a powerful and yet overlooked common effect, which is mental health. Even in the absence of an obvious adversary, compromised mental health poses serious risks to individuals and their units. For example, the scenario named "Private Jane's Secrets," raises

questions about leadership's role in monitoring and controlling online behavior.

Jane's secret online life and shocking response raises unsettling questions for leaders. For instance, it leads to the question, "Should federal agencies and the armed forces draft online codes of conduct and intervene more aggressively in personnel's virtual personas, given the potential effects on their ability to perform their duties?"

In addition, individual and unit readiness is traditionally addressed through physical fitness and skills-based training. Given the mounting urgency to address mental health, there is a pressing question on how federal agencies, including military and law enforcement, should both proactively invest in the psychological fitness of front-line forces and provide them and their families with the resources to recover following an attack.

Although some efforts have been made to address mental health concerns, particularly in response to the recent COVID epidemic, it would benefit the government to develop its own capabilities and competencies with a focus on mental health, especially given the near-infinite attack surface transitive data poses now and in the future.

PRIVATE JANE'S SECRETS

Future Private Jane is the armorer for a U.S. Army training unit, whose secret life in virtual reality is as thrilling as her days on base are boring. In the metaverse, she can be anyone and everyone – or so she believes, until she learns her own likeness is now the best-selling virtual avatar "on the base." The unit's chaplain then misuses footage from his tele-counseling sessions to create evocative videos for sale on the Internet. Emotionally devastated by this revelation, she plots revenge, which is her own livestreamed suicide in the armory during inspection. In the public uproar following, her entire unit, from the command staff down to her squad mates, is deemed temporarily unfit to serve.



Finding 4: Attacks on HVIs in the business and financial communities

Criminals and foreign adversaries will target prominent figures in business and finance to manipulate markets and destabilize the U.S. economy and financial systems.

Over the last decade, the rise of in-game virtual economies, universal payment systems, crypto- and digital currencies, such as Bitcoin and the proposed “digital dollar,”³⁶ as well as blockchain-based tokenized ownership of digital assets together have created exciting new business opportunities. At the same time, they have introduced vulnerabilities into the broader U.S. economic system. This is the result of new and more opaque virtual assets mixing with traditional economic elements, increasing the probability of attacks.

The example of the rise-and-fall of FTX underscores the velocity and size just a handful of actors can achieve with digital assets. A Bahamas-based cryptocurrency exchange, FTX was worth \$40 billion before its founders were accused of fraud after losing \$8 billion of customer deposits.³⁷ The firm’s collapse and subsequent fears of proliferation to other cryptocurrency exchanges and the banking system also highlight the dangers of transitive financial data, because these assets are rapidly

correlated with other instruments.

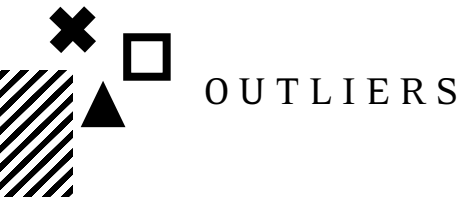
Adversaries seeking to harm the financial system and economic health of the United States will target principal figures at these firms, by either attempting to gain access to accounts and critical systems, or by using disinformation to destroy their personal reputations and trust in their institutions. Others may use false customer accounts (“sock puppets”) to perpetuate fraud or launch Trojan Horse attacks. Long-game operations might also include the creation of entire front companies and currencies with the aim of controlling and destroying critical nodes in the virtual financial system.

Finally, the ongoing evolution of in-game economies and other parallel financial systems within virtualized spaces will create new opportunities for criminal activities, such as money laundering and fencing stolen digital assets. These may, in turn, be used as invisible incentives for attackers to cultivate insider threats. It will be necessary to continuously map and understand the ever-changing patterns of these emerging parallel economies.

³⁶ Alondra Nelson, Alexander Macgillivray, and Nik Marda, “Technical Possibilities for a U.S. Central Bank Digital Currency,” Published on September 16, 2022 by The White House, <https://www.whitehouse.gov/ostp/news-updates/2022/09/16/technical-possibilities-for-a-u-s-central-bank-digital-currency/>.

³⁷ Kalley Huang, “Why Did FTX Collapse? Here’s What to Know,” The New York Times, (November 10, 2022), sec. Technology, <https://www.nytimes.com/2022/11/10/technology/ftx-binance-crypto-explained.html>.





This section covers two ideas that emerged outside of the primary finding categorizations. Outliers constitute an instance of a future threat that appeared perhaps in one fictional future, but not cleanly enough with other models to create a pattern. However, outliers also indicate novel thinking that challenges traditional projected paths and may illustrate “black swan” events that require more attention. Due to their uncommon nature, solutions to outlier challenges are much harder to evaluate.

Outlier 1: Simulated infamy and the loss of reputational sovereignty

The combination of transitive data and increasingly powerful generative AI is expected to result in the loss of control over an individual's image, reputation, and identity.

A historical vignette provides context for how a person might lose control over their image, reputation, or identity. On July 27, 1996, a security guard, Richard Jewell, discovered a backpack containing three pipe bombs concealed on the grounds of Atlanta’s Centennial Olympic Park. Jewell helped evacuate the area before the bombs exploded, saving many from death and severe injury. Nonetheless, he became a person of interest to local law enforcement and the Federal Bureau of Investigation, leading to rampant speculation of him being responsible for the planned attack, until he was finally cleared by the Justice Department. Following a long and bitter struggle with the media, Jewell finally succeeded in restoring his reputation.

But one set of facts wasn’t questioned. Jewell was in the park. He did discover the bombs. He did assist in the evacuation. The verifiability of these facts and general cultural consensus of their veracity enabled him to clear his name. None of these variables can be expected in future events.

The advent and rapid evolution of generative AI audio, visuals, and text will inevitably be combined with individuals’ transitive data to create digital replicas that can be inserted into virtually any kind of media.

Additionally, the ramifications have the capacity for greater damage than deepfakes. Replicas that are legitimately sourced, scraped, stolen, or even counterfeited, may be used to degrade an individual’s public image, and also affect their sense of self and mental health.

Unlike Richard Jewell, whose physical presence in Centennial Olympic Park helped prove his innocence, which ultimately gave him the designation of a hero, ordinary individuals in future different, and virtual environments, are more likely to be found guilty through no fault of their own. Use of advanced AI may allow adversaries to blur reality to the point where “facts” cannot be verified.

Domestic and international populations are ill-prepared for the coming psychological consequences of losing sovereignty over their own actions. Unfortunately, that day has already arrived.³⁸ The question that needs to be addressed is “what to do about it?”

³⁸ Asia Grace, “I Was in Deepfake Porn, Fans Think It’s Real — It Can Happen to Anyone,” New York Post (February 24, 2023), <https://nypost.com/2023/02/24/i-was-in-deepfake-porn-fans-think-its-real-it-can-happen-to-anyone/>.



Outlier 2: AI creates tangible new (un)realities

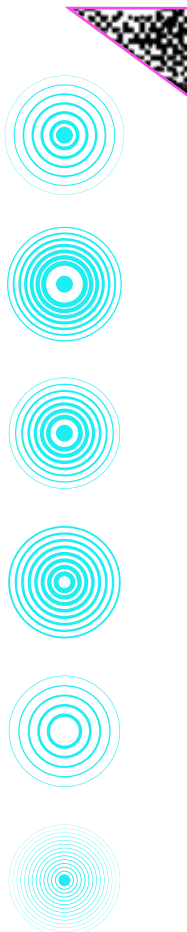
Just as the combination of generative AI and transitive data will lead to realistic replicas of people, it is projected to also be employed to create uncanny replicas of places, situations, and attacks.

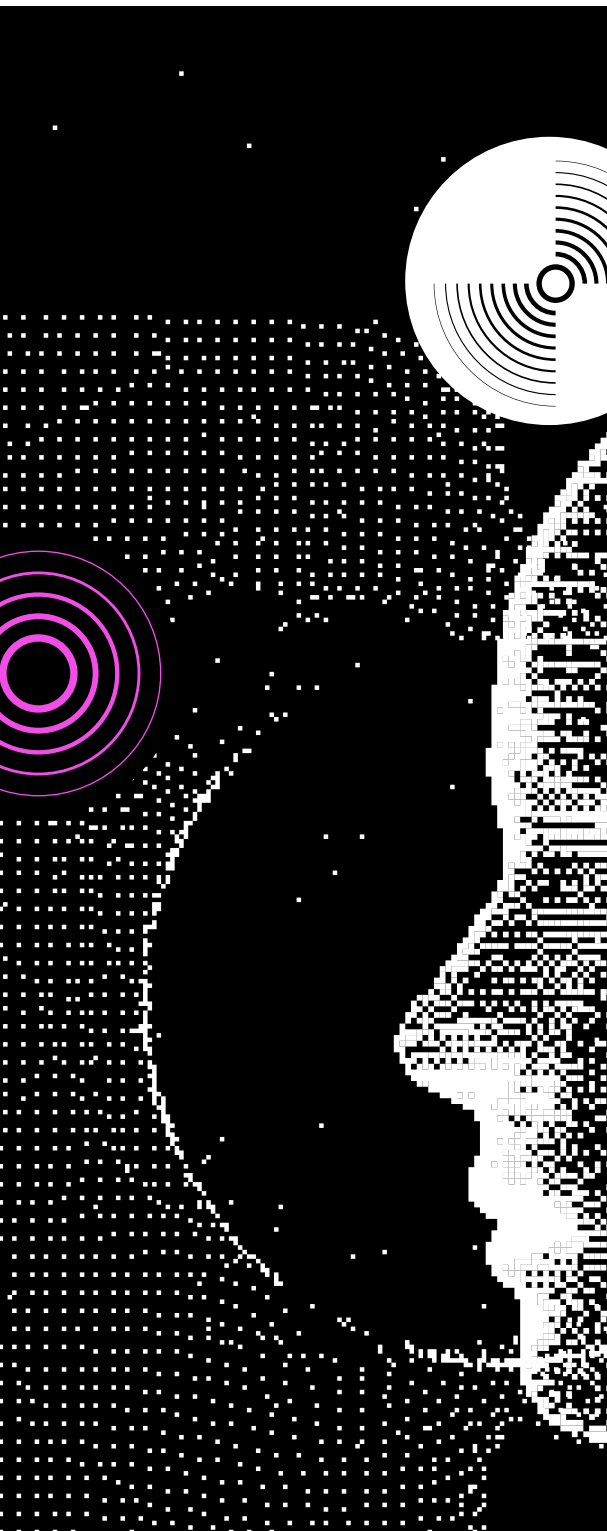
As an example, in November 2022, a Connecticut judge ordered *Infowars* conspiracy broadcaster, Alex Jones, to pay the families of eight children murdered in the 2012 Sandy Hook Elementary School shooting. Jones was charged with \$473 million in punitive damages for defaming them, on top of the \$965 million in compensatory damages awarded by a jury a month earlier.³⁹ For years, Jones claimed the shooting was a “false flag” operation by law enforcement and that the families were “crisis actors.” This led to years of abuse, confrontations, and death threats. In addition, both cases found that at no point did Jones *believe* the lies he was spreading.

As a generative AI and transitive data situation, consider what it would take to fake a school shooting. What is unknown is how much data would be required to do this convincingly, yet likely the combination of generative AI and transitive data will lead to digital replicas of people, allowing the same techniques to be used to create replicas and fabrications of events and situations. In one fictional future, it was imagined that a bad actor hacked into a school’s public address system to sow confusion and panic with deepfake announcements of a shooter, with an order to shelter in place. In this scenario, deepfake calls to 911 and other authorities created substantive digital evidence of an attack-in-progress and deepfake social media posts created the appearance of victims and missing children. Much of the technology needed for this type of attack is presently available.

In this scenario, it would be difficult to determine whether it was microtargeting or another type of attack. Also, it would be extremely challenging to know how the target would be determined and what the motive would be. The ominous answer is the culture’s shared reality. Even after this particular fictional event was debunked, some would likely believe there had been a shooting, just as some *Infowars* viewers believed Jones’ wild accusations. In such cases, microtargeting attacks will create the basis for future disinformation, which will in turn, further degrade the public’s ability to trust that the government will protect them.

³⁹ Associated Press, “Alex Jones Ordered to Pay \$965 Million for Sandy Hook Lies,” Published October 12, 2022 by CNBC, <https://www.cnn.com/2022/10/12/alex-jones-ordered-to-pay-965-million-for-sandy-hook-lies.html>.





Introduction

It is important to trace how the four threat areas are expected to manifest over time and identify how gatekeepers will be able to address them. To that end, there are a series of indicators or flags worth watching out for, which are typically outside of a gatekeeper's control. The exploration of indicators and trends that naturally appear due to market forces, socio-economic forces, political trends, and the natural ebb-and-flow of human progression shapes our understanding of the pathways that lead to specific futures emerging. Flags are guideposts to both preferred and non-preferred futures, so it is imperative that the reader understands the context of an emergent flag to their own organization or application area.

Flags offer early warnings and clear signals that a specific threat is about to occur. They are timed in a way that prevents organizations from reacting too early or late to global events. Even though their timing is precariously designed, their signals appear as fundamentally clear, observable, and quantifiable evidence, upon which strategies can be built.

The following list of indicators and actions have been applied to each of the four main findings. The intention of the authors is to create a roadmap for identifying flags and intervening as early as possible to emergent threats, vulnerabilities, and risks.

Technological Progression

Microtargeting, by nature, is built on the backbone of transitive data, personal, professional, and civil hardware platforms as well as public and private networks. The progression of these technologies over the next decade are expected to primarily occur in private industry and be driven by commercial market forces.

Microtargeting actions will likely be enabled by a variety of comprehensive developments in technology. A brief description of the primary technology trends is provided below.

Developments in Hardware and Software, including:

- ▶ Widespread acceptance, proliferation, and access to cloud storage.
- ▶ Ongoing development of large language models for AI/ML (machine learning) and autonomous software technologies.
- ▶ Increasing development, acceptance, use, and monetization of biometric authentication.
- ▶ Increasing development, acceptance, use, and monetization of personal, professional, industrial, commercial, and civic IOT systems.
- ▶ Development and mainstreaming of neuro stimulators, body mods, and “self-optimization” technologies that are commercially available, yet unregulated.
- ▶ Privatization of medical devices, such as monitors and prosthesis, etc. that result in limited checks and balances.

Expansion of Transitive Data Systems, including:

- ▶ Widespread integration, collection, and monetization of a person’s financial, personal, and professional profiles into a collective identity.
- ▶ Expansion of data acquisition across multiple fields by private firms offers access to a wider range of data that was originally collected for commercial purposes. Examples include grocery stores, supply chains, social media, Personally Identifiable Information (PII), and medical records, etc.
- ▶ Pervasiveness of social media that reveals latent connections to individuals, making them potential targets or proxies.
- ▶ Increasing use of data generated by and for AI, chatbots, and relationship computing devices that reflect the “personal” relationship a single person has with multiple AI systems.

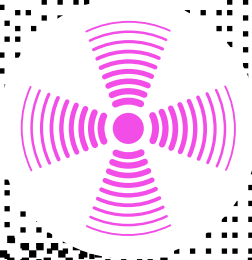
Economic and cultural reimagining of “value” proxies, such as follower counts, likes, subscribers, social credit scores, non-fungible tokens (NFTs), and digital collectibles. This includes:

- ▶ Increasing the value placed on a person’s status in a digital realm, such as on social media or in a virtual environment.
- ▶ The improvement and spread of various forms of social hierarchies, which are often informed by a quantitative “score” that allows access to various tiers of convenience or service based on the person’s score.
- ▶ Rapid adoption of NFTs or digital collectibles with tradeable value in the “real world.”

The Three Sides of Next Generation Security

Given these technological developments, new forms of security will be necessary to protect individuals, including HVIs, vulnerable citizens, soldiers, and federal employees. This will become evident as microtargeting is defined by its misuse and the harm inflicted on individuals, institutions, and society. Natural social evolution and market forces will be areas in which new forms of security are necessary.

Both positive uses and possible misuses of security improvements can be tracked to monitor the progression of microtargeting capabilities, target vulnerabilities, and risk pathways. Some of the following indicators appear to fall within the control of gatekeepers and organizations, such as federal law enforcement agencies and the military. However, it is anticipated that many of these improvements will require additional work outside of federal forces. Each set of indicators below contain a brief description with examples.



Safeguarding methods to improve protections include:

- ▶ Enhanced personal protection and broader regulations surrounding privacy and synthetic biology applications, as well as synthetic biology supply chain monitoring and auditing.
- ▶ Upgraded synthetic biology regulations, such as the regulation of how IoT-based biological data is collected.
- ▶ Creation of bioactive encapsulation technology regulation that is designed to keep bacteria and viruses viable for transportation or deployment in a weaponized form.
- ▶ Enhanced legal and privacy protections that surround facial recognition and machine-automated surveillance.
- ▶ Creation of policies that are designed to tighten restrictions around the collection and retention of data.
- ▶ The establishment of norms for legal liability if someone does *not* use enhanced or virtual tools, especially in such areas as medicine, the military, and law enforcement.
- ▶ A growing understanding that human-machine pairing, likely based on AI/ML, is more capable than humans alone.
- ▶ The emergence and use of improved software auditing, such as a software bill of materials.
- ▶ The possibility of legal liability for not using “enhanced” reality medicines (e.g., trailing regulation has been effective and would protect organizations from harm).

Primary threats to look out for and new methods outpacing detection and/or prevention efforts, include:

- ▶ Adversaries opposing improvements on protections proposed by legal precedence, lawmakers, or communities of interest. By slowing down regulation and oversight, adversaries may have more time to discover new attack vectors unaffected by protection efforts.
- ▶ Microtargeting U.S. targets outside the U.S., such as people, organizations, values to evade local protections, norms, and tools.



Advanced threats to look out for and how to enforce civil control with AI/ML tools, include:

- ▶ The convergence of advanced surveillance tools coupled with AI/ML to analyze and integrate with data from other transitive data sets. As an example, China is expected to deploy these technologies on its own population through “social credit scores” and “COVID-Zero” lockdowns, along with exporting such tools for use elsewhere. Although the latter is not explicitly a driver in any of the Threatcasting models in this report, separate research shows that this is happening.⁴⁰
- ▶ The emergence of AI/ML algorithms to detect patterns of broad civil unrest.
- ▶ The control of soldiers’ and law enforcement professionals’ access to social media.
- ▶ The Chinese government Ministry of State Security (MSS) active monitoring of people-of-interest database and MSS-to-operations pipelines.
- ▶ Nation states sponsoring more interference.

Degrading Economic and Social Conditions Lead to Vulnerabilities

We argue that influencing vulnerable populations will be a key component of future microtargeting operations. Groups that experience the following events may be more susceptible to stochastic terrorism and insider threat development activities.

- ▶ Long-term declines in confidence in U.S. institutions, including the military and law enforcement, and other federal government agencies.⁴¹
- ▶ Increasing U.S. political polarization that undermines community bonds and trust in others.⁴²
- ▶ Falling U.S. life expectancy unevenly distributed across race and gender.⁴³

⁴⁰ Jason C. Brown et al., *Powerful Narratives: Weaponized Harmony and the Soft Power Tools of China’s Rise to Global Primacy* (West Point, NY: Army Cyber Institute, 2022).

⁴¹ Jones, J. M., “Confidence in U.S. Institutions Down; Average at New Low,” Gallup, Published July 5, 2022, <https://news.gallup.com/poll/394283/confidence-institutions-down-average-new-low.aspx>.

⁴² Zacc Ritter, “Polarization May Undermine Community Bonds, Trust in Others,” Gallup, Published February 19, 2020, <https://news.gallup.com/opinion/gallup/284357/polarization-may-undermine-community-bonds-trust-others.aspx>.

⁴³ Elizabeth Arias et al., “Provisional Life Expectancy Estimates for 2021,” Vital Statistics Surveillance Report, (August 2022), <https://www.cdc.gov/nchs/data/vsrr/vsrr023.pdf>.

- ▶ Rising U.S. mortality rates, including maternal mortality rates⁴⁴ unevenly manifesting by race, and working age mortality rates attributed⁴⁵ to an increase in deaths due to alcohol, drugs, and suicide (e.g., “deaths of despair”).⁴⁶
- ▶ Rising U.S. income inequality that is driven by declines in bottom-tier income.⁴⁷
- ▶ Lack of income and opportunities that lead to violent extremism in the Global South, an international relations term that divides the richest and poorest nations.⁴⁸
- ▶ Political polarization that threatens U.S. military and law-enforcement agencies’ recruitment, training, and cohesion capabilities.⁴⁹

Expansion of New Influencer Types

The future of influence may evolve to include new types of influencers and new sources of influence. We posit that successful microtargeting operations may include additional reinforcement by trusted, popular, or “information bubble” personalities, including those that are completely digital and/or AI-controlled – with those who have political and financial influence.

Novel technologies will likely enable the emergence of political “influencers.” These influencers are expected to explicitly use their followings to offer commentary and mobilize activism without holding political office. They could be a previously non-political influencer who is motivated (or radicalized) to switch from commercial to political messaging.

Corporate competitors, are another example, as they are expected to strive to build their own better tools to detect and report a competitor’s malware to garner positive reputations as “defenders” and/or for commercial gain.

⁴⁴ Donna L. Hoyert, “Maternal Mortality Rates in the United States, 2021,” Centers for Disease Control and Prevention, Published 2023, <https://www.cdc.gov/nchs/data/hestat/maternal-mortality/2021/maternal-mortality-rates-2021.htm>.

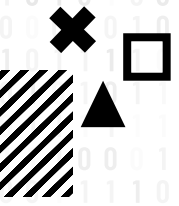
⁴⁵ Farida B. Ahmad et al., “Provisional Drug Overdose Data,” National Center for Health Statistics, Published March 6, 2023, <https://www.cdc.gov/nchs/nvss/vsrr/drug-overdose-data.htm>.

⁴⁶ Elisabet Beseran et al., “Deaths of Despair: A Scoping Review on the Social Determinants of Drug Overdose, Alcohol-Related Liver Disease and Suicide,” *International Journal of Environmental Research and Public Health* 19, no. 19 (September 29, 2022): 12395, <https://doi.org/10.3390/ijerph191912395>.

⁴⁷ Jessica Semega and Melissa Kollar, “Increase in Income Inequality Driven by Real Declines in Income at the Bottom,” *United States Census Bureau*, (September 13, 2022), <https://www.census.gov/library/stories/2022/09/income-inequality-increased.html>.

⁴⁸ “Hope for Better Jobs Eclipses Religious Ideology as Main Driver of Recruitment to Violent Extremist Groups in Sub-Saharan Africa,” *United Nations Development Programme*, Published February 7, 2023, <https://www.undp.org/press-releases/hope-better-jobs-eclipses-religious-ideology-main-driver-recruitment-violent-extremist-groups-sub-saharan-africa>.

⁴⁹ Stefan Borg, “Meeting the US Military’s Manpower Challenges,” *The US Army War College Quarterly: Parameters* 52, no. 3 (August 25, 2022), <https://doi.org/10.55540/0031-1723.3171>.



GATES

Organizations can begin to act in response to emerging microtargeting threats, tools, and outcomes. Many actions can be taken early enough to disrupt the threat before it occurs. By using the indicators above as signals of a threat's progression, organizations can make decisions about when and where to invest time and effort to mitigate and recover from the threat.

Analysis of the data gathered suggests federal law enforcement agencies and the military should proactively invest in three key areas: digital defense, human protections, and education. A description of how to address each key area is provided below.

Develop an Advanced Digital Defense Posture

Creating an updated defense posture that accounts for microtargeting risks requires rethinking cybersecurity with a focus on how *transitive data* and risks affect HVIs, federal populations, and vulnerable populations. Recommended steps to take include the strategies and tactics listed below.

Modernize risk management to move beyond threat detection toward mitigation, recovery, and resilience.

Modernize defense, detection, and intelligence pace and scope. The primary actions defenders could take in this area include enhanced testing of autonomous technologies, purposeful efforts to identify microtargeting tactics, and illuminating layered and convergent transitive data systems.

Prepare and train defenders for transitive attacks. Defenders must accelerate their learning cycles to keep pace with, and get ahead of, the speed and scale of adversarial attacks. This will require rigorous testing, using automated detection in appropriate places within technological and data systems, and fully understanding how technologies are layered. It will also require the testing and automated detection of holes within each additional layer to uncover new forms of vulnerabilities and understand how cryptocurrency systems function.

Encourage and enforce rigorous testing of autonomous technologies. Tactics include:

- ▶ Rigorously testing autonomous technologies (e.g., AI/ML-driven software, robotics for military and sensitive missions) to identify and uncover

vulnerabilities in these systems, such as security weaknesses, decision-making biases, and exploitable software and hardware supply chains.

- ▶ Working with private industry to explicate large language models and ensure integrity of AI assistants and autonomous technologies.
- ▶ Encouraging standards bodies such as the National Institute of Standards and Technology and the International Organization for Standardization to set safety standards for autonomous technologies.

Monitor and detect automated targeting efforts. Tactics include:

- ▶ Increasing interagency collaboration to plan and develop capabilities to detect, identify, and neutralize future cybercrime and extortion threats to U.S. citizens. An example of this occurred when in 2022, representatives from the Army Cyber Institute and the U.S. Secret Service reported on the future of cyber-enabled financial crimes.⁵⁰ Microtargeting tactics are closely related to various economic and financial crimes.
- ▶ Monitoring and detecting patterns of suspicious and malicious cryptocurrency activities.
- ▶ Investing in research to identify deepfakes at the speed and scale of anticipated growth in AI/ML toolsets and models.
- ▶ Closely monitoring politically polarized rhetoric that is intended to undermine public trust in federal agencies and institutions.
- ▶ Continued focus on reporting of foreign travel, activities, and interactions to U.S. law enforcement or counterintelligence agencies upon return to avoid blackmail scenarios.

Develop capabilities to detect radicalization and recruitment campaigns that target individuals or groups. Tactics include:

- ▶ Continuing to fund and expand threat evaluation sources and methods.
- ▶ Understanding and evaluating the social and legal tensions surrounding AI-generated text, images, and videos potentially endangering the safety of children.

Research and understand the convergence of many-layered tech and transitive data systems. Tactics include:

- ▶ Exploring norms and regulations on how transitive data is used by AI/ML and other autonomous technologies.
- ▶ Exploring forensic techniques to conduct counterintelligence operations against adversaries that try to exploit transitive data vulnerabilities.
- ▶ Developing the capability and regulatory apparatus to monitor and scan virtualized spaces that range from multiplayer games to immersive environments.

⁵⁰ Brian David Johnson et al., *The Future of Cyber Enabled Financial Crime: New Crimes, New Criminals and Economic Warfare* (Arizona State University, 2022).

- ▶ Developing enhanced-reality-blended tools (e.g., biomarkers, digital twins in the metaverse) for constructing virtualized spaces, with the goal to simulate possible and probable effects on HVIs and other vulnerable populations.

Detect insider threat risks at scale. Tactics include:

- ▶ Continuing to update insider threat programs to identify and evaluate potentially vulnerable employees. Move beyond awareness training to develop and implement support systems that provide a trusted and safe outlet for military and law enforcement organizations to seek assistance and self-report external stressors and risk factors.
- ▶ Bolstering the identity and reputation management organizations and services within medical, corporate, and federal institutions.
- ▶ Developing support systems that assist employees in getting help to protect against and recover from being a victim of targeting. This will require mirroring how the credit industry monitors credit card access and fraud recovery.
- ▶ Developing support systems that assist organizations in getting help to protect against and recover from being a victim of targeting.
- ▶ Conducting further research to understand the vulnerabilities and associated risk profiles of mental health, as a focus of microtargeting techniques.

Develop controls and detection for cryptocurrency market vulnerabilities.

Invest, research, and explore AI/ML health-related and medical threats to HVIs, federal employees, soldiers, and other vulnerable populations.

Create AI-aided content moderation and oversight. Tactics include:

- ▶ Controlling information flow to limit and counter the spread of disinformation.
- ▶ Researching and developing a plan to use AI-aided content moderation on public communication venues; not a recommendation for blanket surveillance and censorship, but a plan to enable industry, academia, and government concurrence on Internet and social media safety.
- ▶ Partnering with industry and academia to develop self-regulation standards in the development of AI tools that can monitor social media content and other places from which microtargeting tactics often emerge.
- ▶ Reducing the cognitive load of responding to the overwhelming number of links that appear in people's emails, such as phishing attempts, which are a common vector for cyber attackers.

Strengthen cybersecurity practices. Tactics include:

- ▶ Bolstering the adoption of proper cybersecurity procedures through cultural change.
- ▶ Adopting stricter guidelines for commercial partners and government agencies for cybersecurity.

Evaluate and update physical security measures. Tactics include:

- ▶ Securing supply chains to reduce reliance on sensitive locations and uses.
- ▶ Advocating for using only domestically produced technologies in sensitive locations.
- ▶ Partnering with private industry to develop a process for fully vetting vendors and new technologies.

Develop and enact regulations and controls on drones and robotics. Tactics include:

- ▶ Creating drone and urban robotics registries for greater traceability.
- ▶ Expanding and improving airspace monitoring, including no-fly zones for large events.

Use Human Rights as a Security Measure

Protect human rights. Tactics include:

- ▶ Increasing and protecting human rights as a security measure beneficial to national security.
- ▶ Establishing personal identity and data sovereignty as a human right.

Define technological benefits for the main population, not only powerful institutions. Tactics include:

- ▶ Government agencies being first to develop and create new lens tech (wearable or implantable) and providing it to citizens.
- ▶ Exploring regulations on how much data a single institutional entity can control.
- ▶ Considering regulations on what types of individual data collection is allowed.
- ▶ Developing technologies that address possible isolation effects of those using AI companions (e.g., seniors, children, vulnerable populations). With this, using shared standards and norms instead of regulations that could be accepted without an onerous review process.
- ▶ Providing critical family support services on-site at government facilities (e.g., childcare, accounting, legal) to insulate and protect military personnel and federal employees from attacks and disruption.

Better understand drivers of mental health/suicide. Tactics include:

- ▶ Building social media threats into current training.
- ▶ Measuring effectiveness of the use of societal norms in suicide education and prevention.
- ▶ Conducting after-action debriefs that include psychological factors (i.e., the mental and/or unseen impacts of a physical threat, such as a fire or active shooter).

Expand Education

Educate HVIs, federal employees, and service members on manipulation and influence factors. Tactics include:

- ▶ Informing the public, private sector, academia, and government across all levels about potential vulnerabilities to manipulation and influence (e.g., general population, social media companies, law enforcement, and even politicians and decision-makers).

- ▶ Exploring and educating people and institutions on how influence and manipulation operations occur, how to detect them, and where to seek assistance.
- ▶ Creating services and programs to assist microtargeted individuals in recovering from attacks. Public Service Announcements (PSAs) with public officials, such as those focused on fire mitigation or active shooter awareness, and statements that address the possible misinformation being spread over social media.
- ▶ Developing individual leadership's awareness on the connection they have to their own technology and understanding its effects.
- ▶ Setting and verifying the integrity and accuracy of mass public notification systems (e.g., emergency channels, Amber alerts, school notification alerts, and Emergency Broadcast System, etc.).

Research and normalize virtual identity rights. Tactics include:

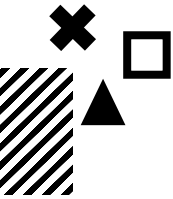
- ▶ Participating in international organizations' ongoing research on defining a person's virtual identity rights. An example is the World Economic Forum's exploration of identity rights in the area of emerging technologies.⁵¹
- ▶ Ensuring that virtual identity rights and norms protect human rights rather than inhibit them.

Develop reputation management products. This will require an understanding of the industries that will develop around these products, which may involve comprehensive identity scraping and personal interviews to assess current and future attack surfaces of clients.

Educate federal employees about how adversaries might use AI/ML and other technological capabilities. Tactics include:

- ▶ Specifying nefarious actor techniques and procedures in education forums that go beyond "awareness training." This will involve creating systems and organizations for employees to have hands-on experience with technological risk factors in a safe and controlled environment.
- ▶ Involving psychologists and mental health care professionals in the education processes.
- ▶ Collaborating with law enforcement training schools to understand how deepfakes can be utilized to commit crimes.

⁵¹ Marcus Bonner, "Why We Need to Regulate Digital Identity in the Metaverse," World Economic Forum, (December 5, 2022), <https://www.weforum.org/agenda/2022/12/digital-identity-metaverse-why-we-need-to-regulate-it-and-how/>.



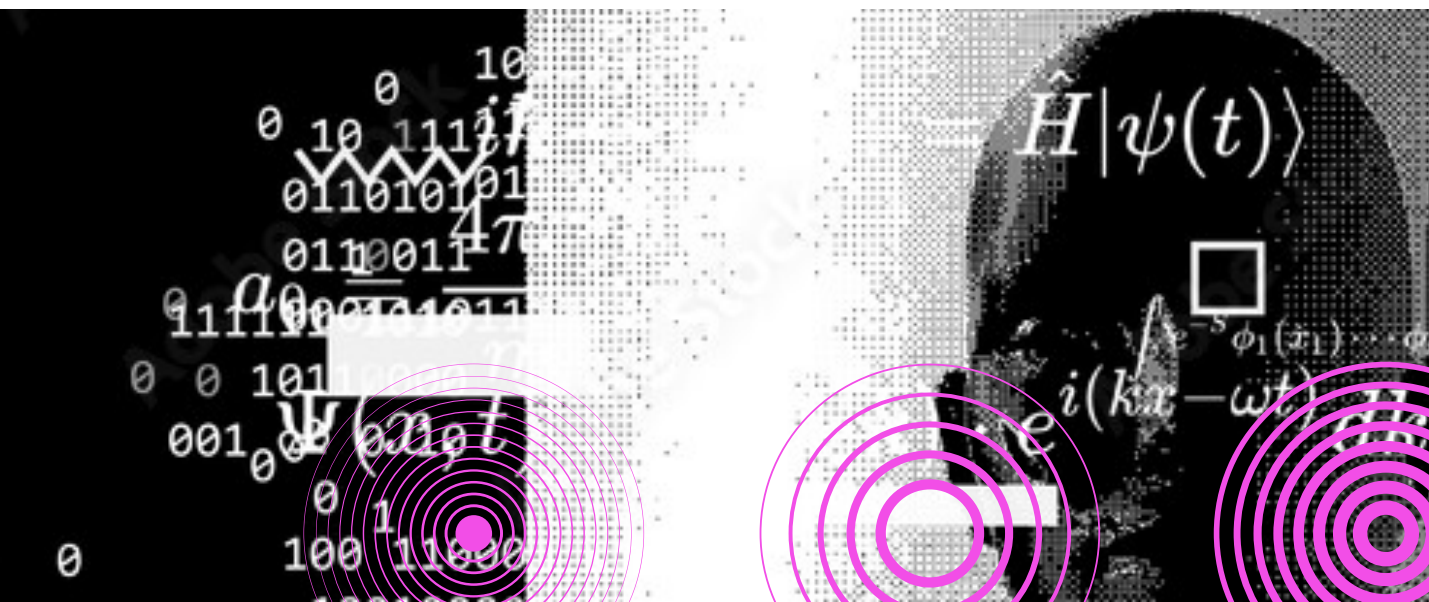
SUMMARY

In the future, bad actors will likely use microtargeting techniques to threaten the missions of federal law enforcement and the military, as well as social and financial structures.

This report has addressed the potential impact of microtargeting on the military, law enforcement, and political leaders in the context of an increasingly interconnected environment. The research questions aimed to investigate the manifestation of microtargeting threats over the next decade and its implications for national defense, the protection of U.S. leadership, and the security of the U.S. economy. In it, there were key threats identified to national security arising from adversaries' ability to exploit data oceans,

identify individuals at scale, and manipulate them for their objectives.

Microtargeting involves the collection and analysis of personal data to create highly tailored messages for advertising, marketing, and influence campaigns. Adversaries seek to destabilize federal institutions responsible for safeguarding the population by targeting high-value individuals (HVIs) in the military, law enforcement, and within civilian leadership. These adversaries seek to stigmatize, extort, and even assassinate crucial figures necessary for the security and stability of the United States. They may also exploit individuals connected to HVIs when direct access to the HVI is not possible.



Adversaries are expected to extend their microtargeting tactics beyond HVIs to include vulnerable subsets of the population, exploiting grievances and fostering division through disinformation. This strategic approach is intended to provoke societal unrest, political dysfunction, and division to gain a strategic advantage. Federal employees, military personnel, and their loved ones are also likely targets, as adversaries seek to influence, radicalize, and weaken the effectiveness of the U.S.'s full fighting force.

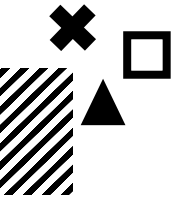
Furthermore, both state and non-state adversaries may employ microtargeting to attack HVIs in the business and financial sectors, manipulating markets to undermine trust in the U.S. economy and its financial system.

To counter microtargeting attacks, advanced resources are required to assist HVIs and those closest to them. Mitigation and recovery strategies include training individuals to recognize such attacks, real-

time detection and countering of deepfakes and disinformation, reputation recovery programs, and exploring mental health solutions to enhance cognitive resilience against microtargeting attacks.

Both historical lessons of cigarette marketing in the 1920s and 1930s and future fictional scenarios provide examples of microtargeting tactics, targets, and consequences. This report does not have all the answers to avoiding, mitigating, or recovering from such attacks, but it does provide federal law enforcement and the military an opportunity to say, "I recognize this!" when encountering future threats.





APPENDIX A

Engineering Consent: An Early 20th Century Guide to Manipulating the Masses

February 27, 2023

By J.H. Carrott

Introduction

The world took a dramatic turn in the early 20th century, as modern technologies spread through American society, accelerating mass communication at a rapid rate. Electricity, film, radio, and eventually television changed the landscape of culture. The scale and complexity of mass media audiences called for new ways of imagining the world and for changing it. This complicated new media environment provided seemingly limitless possibility for communication and control. At the same time, it took more than physical technology to take advantage of all this new, electric modernity had to offer. Truly effective manipulation, enabling completely new strategies, would require new ways of thinking.

Public relations pioneer Edward Bernays thought he had an answer to manipulating minds in this newly complicated age. His method, in many ways a technology in itself, focused on the effective leveraging of information and context. The piece below examines his work during the 1920s, leading to his work for Lucky Strike cigarettes.⁵² Bernays' story, and that of one of 1928's most popular publicity campaigns "Reach for a Lucky instead of a sweet!" provides great illustrations of what Bernays called the "engineering of consent."

The Engineer

Edward Bernays was not shy about reminding people of his connection to his famous uncle Sigmund Freud. Bernays is also justly credited with founding the modern discipline of public relations, which he thought of as a way of using propaganda methods in peacetime.⁵³ He had a very modern answer to the very modern question of manipulating the human mind. He called it the "engineering of consent" and it changed how most of us think, whether we are aware of it or not. In an excerpt from his 1928 book, *Manipulating Public Opinion: The Why and The How*, Bernays casts the changing of the public mind as a technical problem:

The innovator, the leader, the special pleader for new ideas, has through necessity developed a new technique—the psychology of public persuasion. Through

⁵² Bernays had a very long career. I set the limits above to focus the discussion.

⁵³ See Tye, 51-55.

the application of this new psychology, he is able to bring about changes in public opinion that will make for the acceptance of new doctrines, beliefs, and habits. The manipulation of the public mind, which is so marked a characteristic of society today, serves a social purpose. This manipulation serves to gain acceptance for new ideas.⁵⁴

Critically, Bernays' work involves research, not only gathering data, but also learning how to apply it. "Sociology also contributes to his technique," Bernays elaborated. He continues:

The group cleavages of society, the importance of group leaders, and the habits of their followers are part of the technical background of his work. He has methods adapted to educating the public to new ideas, to articulating minority ideas and strengthening them, to making latent majority ideas active, to making an old principle apply to a new idea, to substituting ideas by changing cliches, to overcoming prejudices, to making a part stand for the whole, and to creating events and circumstances that stands for his ideas.⁵⁵

Bernays was also not shy about using the word propaganda to describe his work. In *Propaganda* (1928), he cast the term as a general, pragmatic, and even necessary method, arguing that:

The minority has discovered a powerful help in influencing majorities. It has been found possible to so mold the mind of the masses that they will throw their newly gained strength in the desired direction. In the present structure of society, this practice is inevitable. Whatever of social importance is done today, whether in politics, finance, manufacture, agriculture, charity, education, or other fields, must be done with the help of propaganda. Propaganda is the executive arm of the invisible government.⁵⁶

In the words of Bernays' biographer Larry Tye, "Hired to sell a product or service, he instead sold whole new ways of behaving, which appeared obscure but over time reaped

⁵⁴ Bernays, *Manipulating* (1928), 18.

⁵⁵ Bernays, *Manipulating* (1928), 20-21.

⁵⁶ Bernays *Propaganda* (1928), 83-84. If this sounds a little dangerous being heard through today's ears, that's because it was. These ideas inspired much of the propaganda Adolf Hitler's Nazi party used to gain control of Germany and later most of Europe. After the Second World War, a (slightly) chastened Bernays was careful (though a little strained) to underline the democratic uses of his processes: "The engineering of consent should be based theoretically and practically on the complete understanding of those whom it attempts to win over. But it is sometimes impossible to reach joint decisions based on an understanding of facts by all of the people. The average American adult has only six years of schooling behind him. With pressing crises and decisions to be reached, a leader frequently cannot wait for the people to arrive at even general understanding. In certain cases, democratic leaders must play their part in leading the public through the engineering of consent to socially constructive goals and values..." Bernays (1947), 40-41.



huge rewards for his clients and redefined the very texture of American life.”⁵⁷ Some of Bernays’ clients during the 1920s were:

- ▶ Proctor & Gamble, for whom Bernays promoted soap sculpture as “a national outlet for children’s creative instincts and helped develop a generation that enjoyed cleanliness.”
- ▶ President Calvin Coolidge, who had a reputation as a “sourpuss who appeared to have been ‘weaned on a pickle.’” Bernays arranged a breakfast at the White House for Coolidge, inviting Al Jolson and other popular celebrities. “This unprecedented feast, widely reported in front-page stories throughout the country. It helped to mellow the president’s reputation.”
- ▶ Best Foods Company, makers of salad oils, for whom he “staged an art show of palette oils and palate oils” at a prominent New York art gallery.
- ▶ Beech-Nut Packing, who wanted to sell more bacon. To this end, Bernays arranged “a survey of physicians who urged Americans, as a health measure, to eat heavier breakfasts. To many this meant bacon and eggs.”
- ▶ Hairnet manufacturer Venida, whose business was suffering as the result of a new fashion: short hair styles for women. Bernays found another angle: “We explored the uses of hairnets as a safety measure for women working with machinery, and as a result of public visibility of the idea, several states passed laws making it obligatory for women to wear hairnets under certain working conditions.”
- ▶ In 1929, General Electric and Westinghouse wanted to call attention to the 50th anniversary of Thomas Edison’s electric light. Bernays set about creating an epic, easily sensationalized event, “Light’s Golden Jubilee.” One reporter reveals the true intent of the event by noting that:

On the surface, a truly great man was being honored by a famous industrialist. As a matter of fact, Mr. Bernays was the man who managed and directed the series of dramatic episodes. He was working ‘not for Edison or for Henry Ford, but for very important interests which saw in this historic anniversary an opportunity to exploit and publicize the uses of the electric light.’⁵⁸

Clearly Bernays was an expert at drawing associations and manipulating contexts, but how did he know how to elicit mass adoption of his campaigns and at what time to produce his intended effect? It may have looked like magic to his clients, but Bernays was no sorcerer. His process involved a critical variable that often gets missed amidst

⁵⁷ Tye, 52.

⁵⁸ John T. Flynn, cited in Bernays (1971), 200.

his clever showmanship and skillful misdirection: gathering and analyzing data. To manipulate people, one needs a deep understanding of what causes people to act. "The objective must at all times," he wrote:

...be related to the public whose consent is to be obtained. That public is people, but what do they know? What are their present attitudes toward the situation with which the consent engineer is concerned? What are the impulses which govern these attitudes? What ideas are the people ready to absorb?... The public's attitudes, assumptions, ideas, or prejudices result from definite influences. One must try to find out what they are in any situation in which one is working.⁵⁹

Bernays' most successful and high-profile campaigns were for cigarettes, in particular, American Tobacco Company, maker of Lucky Strikes. The campaigns he developed and the institutions he founded would serve as the basis of one of the biggest non-political deceptions of the 20th century. That story starts with the 20th century's penultimate⁶⁰ consumer good—the cigarette.

"Reach for a lucky instead of a sweet!"

The 20th century's innovations brought an explosion of mass media and consumer culture. Driven by the need to sustain wartime levels of production during the first half of the 20th century, Americans wove mass consumption into the social, cultural, political, and economic fabric of the nation, building what Historian Lizabeth Cohen called the "consumer's republic".⁶¹ Advertising worked to convert and excite the public, urging the masses to consume the multitude of merchandise that American production had to offer. A new way of expression and being expressed through consumer goods began in the United States and swept across the developed world, influencing a comprehensive range of cultural norms from personal hygiene to politics.

Cigarette smoking offered a vast improvement and cleaner alternative to chewing tobacco. In comparison, cigarettes were relatively discreet, sanitary, and very, very modern. Pipes and cigars retained some appeal throughout most of the century, but cigarettes defined the culture of smoking in the 20th century. By the early 1900's, premature illusions about smoking being healthy had dissipated, but cigarettes were still considered the better option for tobacco uses. Anti-smoking efforts in the 19th century had been wrapped up in issues of morality and behavior, often focused on preventing smoking in women and children. Historian Sarah Milov describes how an alliance of "temperance reformers, eugenicists, nativists, and industrial efficiency experts waged war

⁵⁹ Bernays (1947), 46.

⁶⁰ I'd put the automobile at number one.

⁶¹ Cohen makes this case eloquently in *Consumer's Republic* (2003).

on ‘the little white slavers.’” They succeeded in convincing several states to restrict the manufacture, sale, or purchase of cigarettes. The cause of social purity was progressing well. Then the First World War happened.⁶²

As death and destruction swept across the globe, cigarettes rapidly became almost a patriotic necessity. Tobacco sales boosted the American economy and smoking kept idle soldiers sober and occupied. Soldiers were issued cigarette tobacco and rolling papers as part of their rations, and wounded soldiers were given manufactured or “ready-made” cigarettes.

Then the attitudes of reformers themselves changed. In context, smoking became a “lessor of evils,” permitted as a controllable vice that wouldn’t be fair to deny soldiers who, at any moment, might be called upon to storm the enemy. Temperance advocates began to argue that smoking could be an active good if it kept soldiers too busy to commit even worse sins. In Milov’s words, the intention of these reformers was that “like a live virus inoculating recipients against a deadly infection, cigarettes were to vaccinate soldiers ... against more serious types of vice—‘intoxicating liquors and lewd women.’” The YMCA, which had previously joined in the moralistic crusade against smoking, became one of the largest wartime distributors of cigarettes.⁶³

Soldiers returned home as habitual smokers and society welcomed them with enthusiasm. The lesser evil argument, combined with the force of economic necessity, took precedence over the morality movement, and many anti-smoking laws were repealed. This was excellent news for the cigarette industry. The 1920s were a triumphant decade for American consumerism, and the cigarette was the ultimate consumer product—a cheap, disposable, habit-forming commodity that also provided a perfect canvas for the newly-honed arts of packaging and marketing. While the cigarette seemed to be everywhere in public, the industry became increasingly aware that some 50% of the population were not really active customers. If they wanted to really expand their market, they were going to need more women to smoke. That was going to take a little consent engineering.

In the classic form of ego-driven business leaders throughout history, American Tobacco President George Washington Hill had already convinced himself that cigarettes were a great diet aid and had conceived “Reach for a Lucky instead of a sweet!” after seeing a lady in a cab next to him. The beautiful, thin woman drew elegantly at a cigarette holder. Immediately after witnessing this, Hill rushed to his office and deployed his most powerful hired hands with two phone calls. Hill first called his ad agency to spin up their

⁶² Milov, 12-13.

⁶³ Milov, 26-27.

design team—he wanted visuals fast. Next, he called Edward Bernays—he needed to change culture itself.⁶⁴

Bernays knew it was going to take some work to effect a cultural change on the scale Hill desired. He took immediate action, producing a wide-ranging, multi-media story that would illustrate the triumph of the slim, fashionable, and noble over the fat, sloppy, and greedy. Exploiting the growing fashion for slimness, he aggressively enlisted the fashion industry, going so far as to anonymously sponsor a conference on the evolution of the modern idea of beauty, wherein artists proclaimed that the “slim woman w[as] the ideal American type.”⁶⁵ He planted news articles mentioning cigarettes and beauty, and linking the ideal woman to a range of smoking accessories in magazines that Lucky Strike’s target audience read.⁶⁶ These weren’t advertisements and their connection to a cigarette manufacturer was carefully concealed. Bernays was manipulating the environment to shift the perceptions of his targets.

One of the goals of the campaign was to overturn traditional resistance towards women smoking in public. Women’s public roles were at the center of a great controversy and discussion during the 1920s and the cigarette, long a symbol of masculinity, became a cultural lightning rod. Bernays’ response was to lean into the controversy, building product associations that appealed to modern women. His insights often involved pressing on cultural fault lines and social cleavages, which then allowed him to leverage information in the right way to affect his target audience in unexpected ways. “Age old customs, I learned,” Bernays said, “could be broken down by a dramatic appeal, disseminated through the network of media.”⁶⁷

Bernays found a psychiatrist willing to go on the record, with no visible connection to Lucky Strike, that cigarettes were symbols of freedom for women and “a sublimation of oral eroticism; holding a cigarette excites the oral zone... Thus, cigarettes, which are equated with men, become torches of freedom.”⁶⁸ Bernays went straight out and organized a “freedom march” led by smoking debutantes along six blocks of Fifth Avenue. Slipstreaming off the success of the suffrage movement and women’s activism, Bernays connected Lucky Strikes with female liberation, performing a kind of cultural jiu-jitsu to flip the gender narrative around smoking in a way that benefitted his client. Bernays’ approach made liberal use of tactics like this, the “created event,” which manipulated the news to seize narrative momentum. He explained that a good public relations consultant, “not only knows what news value is, but knowing it, he is in a position to make news happen.”⁶⁹

⁶⁴ Kluger, 77-78.

⁶⁵ Many artists were likely paid to attend. Quoted in Brandt, 338.

⁶⁶ Bernays, in Brandt, 337.

⁶⁷ Bernays, in Brandt, 341.

⁶⁸ Kluger, 78.

⁶⁹ Bernays, in Brandt, 335-336.

In American Tobacco's campaign research project, another complication emerged. It was the color green. Female consumers told researchers that the iconic green color of the Lucky Strikes package clashed with their clothing. The color was simply out of fashion. When Hill first brought this problem to Bernays, the savvy promoter suggested the obvious. "Change the color of the package, I suggested. Mr. Hill was outraged. I then suggested we try to make green the dominant color of women's fashions." Bernays' brilliantly covert method was a smashing success, executed in part through a modification of his palette/palate event for Best Foods described here:

For a year we worked with the New York Infirmary for Women and Mrs. Frank A. Vanderlip, its president, to hold a Green Ball, with tableaux of socialites dressed in green based on the paintings of the Malmaison masters in the Luxembourg Museum in Paris. We worked with manufacturers of accessories for dresses and textiles to ensure that gloves, stockings, shoes, and other accessories would also be green. *Harper's Bazaar* and *Vogue* featured green covers of fashions on the date of the Green Ball. Green became fashion's color.⁷⁰

Further cementing his reputation as a wizard of modern media, Bernays proposed in 1929 that the company set up the Tobacco Information Service Bureau (TISB) that could issue news releases and prepared media, helping to drive the narrative from behind the scenes and "provide a certain scientific background for what the Bureau may from time to time say from a scientific standpoint."⁷¹ The idea was to create a mechanism for covertly spreading suspect science to create news and manufacture controversy. The TISB formed the foundation for a whole strategy of indirect influence that the industry exerted for the rest of the century. Science put tobacco on the defensive for a lot of the second half of the 20th century, as more studies featured clear scientific evidence linking tobacco to a wide array of health risks. Bernays himself jumped ship after a 1964 Surgeon General's report that causally linked cigarette smoking and death.⁷²

At that point, rather than attempt to contest a scientific argument, the tobacco industry knew they had no way of convincing the public that smoking was healthy. So, industry leaders chose to sow a different kind of doubt and uncertainty. They launched the Tobacco Industry Research Council. The industry's response to the wave of studies that began coming out during the second half of the century was to think big and indirect like Bernays. They financed a whole ecosystem of alternative science to challenge the mainstream medical consensus. The idea was not so much to convince people that

⁷⁰ Bernays (1971), 195.

⁷¹ Bernays, in Brandt, 336.

⁷² Upon his defection, Bernays made a big deal about a plan to reverse "his wrongs" through a campaign to make smoking "an antisocial act." While he did get involved in some antismoking initiatives, he never managed to apply the kind of focus and genius to a problem that was not paying him a substantial sum. Nye, 49.

cigarettes were healthy, rather it was to give people excuses to set aside scientific conclusions, and confuse perception just enough to support the industry. It held off responses like smoking bans for decades.⁷³

The industry kept up this behavior wherever it legally could, working on historians even into the early 21st century. Medical historian Allan M. Brandt had just begun work on his 2009 book, *The Cigarette Century* when he received an office visit from tobacco industry attorneys who “wanted to know whether there had been any controversy about smoking and health in the 1950s. Were any scientists and physicians genuinely skeptical of the epidemiological studies linking smoking to lung cancer?” Brandt describes his response:

Of course, there was a controversy, and of course there were skeptics. It would be difficult to identify a significant finding in medicine and science that did not attract some degree of skepticism. The lawyers seemed quite pleased with this response. But I went on to explain two additional facts. First, although there truly were skeptics, even a handful who were not associated with the industry, they were a rare breed, and very few had done any original research on smoking and health. Second, the industry had worked diligently to foment the controversy. Without these efforts, the harms of smoking would have been uniformly accepted by medical science long before the 1964 Surgeon General’s report—which, I pointed out, the industry had also sought to trash. The perception of ongoing, heated debate about the relationship of cigarettes and disease had largely been a product of the industry’s intensive public relations efforts in the 1950s and after. Any professional historian, I said, would place the “debates” about the harms of smoking into this context. Suddenly my visitors were not so happy with me. I never saw them again.⁷⁴

Brandt highlighted the context, which was central to the matter. Setting and manipulating the context was an act pivotal to public relations. Bernays’ professionalization of “public relations” even shifted the context on propaganda itself. Propaganda was no longer just a weapon of war; it could be turned on the public. Bernays, ever the manipulator, spun this as democratization in his statement:

Public opinion was made or changed formerly by tribal chiefs, by kings, by religious leaders. Today the privilege of attempting to sway public opinion is everyone’s. It is one of the manifestations of democracy that anyone may try to convince others and to assume leadership on behalf of his own thesis.⁷⁵

⁷³ Brandt, 493.

⁷⁴ Brandt, 493.

⁷⁵ Bernays (1928), 17.

Conclusion

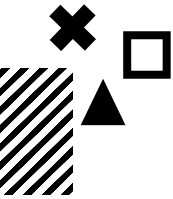
Whether he believed his democratization message⁷⁶ and whether he intended it, Bernays was deflecting attention from a central problem, which was that while anyone could attempt to influence public opinion, not everyone has the necessary resources, access, data, and experience. Those are increasingly the province of nations, well-funded corporations, and organized non-state actors. The elegance of Bernays' work lies in his understanding of his target audience and the pressure points he could utilize to manipulate them. This point bears particular underlining in the 21st century, as information technology has enabled corporations, governments, and almost any organization to target audiences with hitherto unimaginable precision.

The few examples above illustrate the impact of applying tiny amounts of pressure at points of cultural fissure and change. Carefully-crafted stories can leverage a potpourri of cultural imagery to give immense indirect power to an activity or identity. Bernays looked for narratives he could connect with new ways to tell old stories. A clever engineer, he could take a pattern from one area of culture, apply it to another, and take it much further.

Bernays was a very clever and perceptive person, able to intuit remarkably effective campaigns in a pre-digital age. Today's technology can extract patterns from exponentially larger "oceans" of data and can aid in the exploitation of culture with a degree of precision Bernays could never have done with the technology available at the time.

⁷⁶ I assert he did believe it at least at first. Bernays' early writings read more naïve than cynical. But he was made aware in the 1930s of Josef Goebbels' use of his technology. That didn't slow him at all (nor did it slow many, many people from doing things the Nazis were able to leverage—I'm not picking on Bernays for that here). My best guess is that his spin was so good that he spun himself in the process of selling his services. His invocations of democracy feel a little more strained after the Second World War. He loved his work for Lucky Strike, but in the end, just couldn't get himself past that 1964 Surgeon General's report. Bernays had moral boundaries; they were just quite wide.





APPENDIX B

Subject Matter Expert Interviews

Below are excerpts of key ideas followed by full transcripts of each Subject Matter Expert interview. These have been lightly edited for clarity. They are the original words of our experts, extracted with artificial intelligence assistance, and should be read as if they were coming from a video recording.

Dr. Mary Aiken, *Professor of Cyberpsychology and Chair of the Department of Cyberpsychology at Capitol Technology University*. She is a world-leading expert in Cyberpsychology, the study of the impact of technology on human behavior. Dr. Aiken is also Professor of Cyberpsychology and Chair of the Department of Cyberpsychology at Capitol Technology University, Washington D.C.'s premier STEM University.

Excerpt – Key Ideas

The introduction of ideas from cyberpsychology – cyberspace's human elements – is changing warfare as well as society. Social media has become a battlespace for competing narratives, information operations, psychological operations, misinformation, and disinformation. Cyber-behavioral profiling has become an emphasis within law enforcement, examining dark character traits and individuals' actions within cyberspace and their choice of malware tools.

When we look at microtargeting – an activity already prevalent in advertising – it becomes unacceptable when it turns into manipulation. Social media is playing a key role in sedition and subversion, and its harms to youth range from harassment to disinformation. The challenge for law enforcement agencies is to make societies safer in cyberspace. Cybersecurity has overly focused on the technical – and must now address cyberpsychology risks as well.

Full Interview Transcript

Hi, I'm Professor Mary Aiken. I'm a professor of cyberpsychology and head of the Department of cyberpsychology at Capital Tech University in Maryland. This year we launched the first online PhD in cyberpsychology which has been very successful especially with those in government agencies. I'm also an academic advisor to both Europol to the EC3 - the Cyber Crime Center - and to Interpol, the Special Cyber Crime Expert Group.

So, cyberpsychology is an advanced discipline within applied psychology. And there's a need to factor in the increasing importance of this discipline regarding human behavior mediated by technology. So, in this brief segment I'd like to highlight the utility of cyberpsychology in terms of predicting and mitigating microtargeting and data protection threats. So, notably the U.S. intelligence community is turning its attention

to cyberpsychology specifically regarding “cyber-psychological warfare.” In fact, IARPA has just issued an RFI seeking to understand what they describe as cyberspace’s human element and to examine how cyber psychological factors can be used in both offensive and defensive operations.

We see how social media - particularly in the context of current conflict - is serving as a battleground for state and non-state actors to spread competing narratives. In terms of future threats, we need to consider increasingly sophisticated microtargeting by foreign actors - a form of cyber or info warfare - tailored online propaganda, and mis- or disinformation deployed tactically and/or embedded over time.

We also have the growing research area of operational cyberpsychology - a field that supports missions intended to project power in and through cyberspace. How? By leveraging and applying expertise and mental processes and behavior in the context of interaction among humans and machines - what you might describe, or what I describe, as cyber Psyops.

My specialist area is forensic cyber psychology and I’m one of the lead investigators in one of the largest EU projects which is investigating human and technical drivers of cybercrime. So, specific to this research in terms of attacks by means of emerging disruptive technologies, one of our areas of investigation is cyber behavioral profiling. In fact, we’re currently working on a paper which is “Human Drivers of Cyber Crime: A Forensic Cyberpsychology Approach to Behavioral Profiling.” And this work is examining relationships between dark personality traits and malware of choice. It’s one of the first research projects to look in depth at this area amongst other things.

So, what does that mean? So, effectively, a perpetrator’s choice of malware, hypothetically, provides evidence regarding base behavioral traits. That’s the hypothesis. So, how does that work? So, ransomware, like any form of hostage taking - real world or otherwise - is a particularly cruel endeavor. Holding somebody against their will, threatening to collapse a business, holding a health care service or hospital to ransom. Cruel endeavors. So, effectively, we’re looking at the potential relationship between those who score highly on dark tetrad traits, which is a co-morbid cluster involving Machiavellian traits, narcissistic traits, sadistic traits, and psychopathic traits.

So, let’s take the hypothesis a little further and consider another form of malware. So, let’s think about spyware, or creepware, or stalkerware. Then arguably, that’s not so associated or even correlated with dark tetrad, but more likely in a psychological context to be closer to what we would call paraphilias - paraphilias such as voyeurism - so, voyeurism and spyware.

So, this research is a form of investigative microtargeting, if you will, of perpetrators and threat actors in terms of their data, their behavior, and respective pattern analysis. So, in terms of microtargeting, people have always tried to influence citizens - to influence others. Microtargeting has been extensively used in advertising campaigns. However, arguably, influenced by microtargeting becomes unacceptable when it turns into manipulation. So, this tipping point is subliminal in cyber contexts to the point of non-detection.

In 2018, I had the opportunity to meet with Congressional staff to discuss the science of behavioral manipulation online apropos the U.S. Senate Intelligence Committee's investigation into Russian efforts to influence the 2016 U.S. presidential election. I subsequently wrote a paper on this topic titled "Manipulating Fast and Slow." Notably, attribution in cyber context is complex, and as I argued in the paper, the elephants in the cyber room - China and Russia - are consistently named and shamed in an exercise that often resonates with "Roundup The Usual Suspects," while weaker state actors jockey for position trying to become stronger and seeking power status, while non-state actors pursue their idealistic goals, activism. And while technology enterprises social media and social tech operate under the radar with little thought given to their potential aspirations of statehood. So, basically, if you want to launch an investigation then everybody is a suspect.

In terms of broad societal influence and large or small-scale reflexive control it is critical to examine the role of social media regarding sedition and particularly subversion. When it comes to the pervasive and profound influence of social technologies, we are currently witnessing a ticking microtargeting time bomb - a virtual back door - into the developmental psyche of American youth - indeed, international youth.

So, how do we protect youth? It's important to factor in online harms. A spectrum of harm ranging from harassment to disinformation. And important to invest in tech solutions to tech-facilitated harmful and criminal behaviors, which have the characteristics of big data in terms of volume, variety, and velocity, and therefore require AI and ML solutions.

Two of my recent reports informed by cyberpsychology principles that I would like to direct you to. Firstly, the "Cyber Blue Line" - if you are familiar with the "Thin Blue Line," now we have the Cyber Blue Line - which considers how law enforcement agencies are overwhelmed in cyberspace and questions where does responsibility lie in terms of ensuring safe and secure societies in cyberspace?

Secondly, my latest research report titled "Towards a Safer Nation: The United States Safety Tech Market," was published last January, and we actually were invited to brief the White House on this report in February.

The point is, we've had 50 years of cybersecurity. Cybersecurity protects our data, our systems, and our networks. It does not protect what it is to be human online, and therein lies the gap. The potential to target and manipulate humans at cognitive, affective, behavioral, developmental, and social levels. These are the cyber-psychological attack factors.

We want our data systems and networks to be robust, resilient, and secure, but going forward, we also want the humans who operate and use these systems to be psychologically robust, resilient, safe, and secure. Therefore, when investigating microtargeting, it is necessary to broaden the approach to the problem space - to the threat landscape - and take a more macro view, create context in terms of human factors and vulnerabilities, develop cyber situational awareness, and lean into emerging transdisciplinary science such as cyberpsychology.

As the National Cyber Director, Chris Inglis, recently said when it comes to cyber society, the choices we make in cyberspace are important. We are all connected there via the Internet. Therefore, arguably, going forwards, threats are a collective responsibility. As Chris Inglis stated, "Each of us must participate in the defense of all of us." Thank you for your time.

J.H. Carrott, *Historian, Tech Nerd, Game Geek*. Jamie Carrott may have been born a historian, but definitive proof awaits further mapping of the human genome. A self-described tech nerd, anachronist, game geek, fanboy, and contrarian, Jamie has followed an eclectic career path that has gone from the deepest recesses of America's colonial past to the future of gaming and entertainment and nearly everywhere between.

Excerpt – Key Ideas

Microtargeting resembles a panopticon – a prison design where a central eye can view each cell circling the center, turning a huge crowd into individuals. Currently, the ability to segment our society increases the ability to microtarget. The need to count, to manage and control, has been at the center of crises. The ability to collect data now must worry about how to manage the massive amounts of data collected. There is a possibility for AI to be the panopticon – the single eye to view everything. This long process began with writing – offloading information onto pages – and continued with human computers (analysts) to analyze that information. Now it is about shifting the processing from people to technology.

The targeting of Cambridge Analytica was a way to harvest information and create a different candidate for everyone. The candidate – or message, or information – is now

tailored, or microtargeted, to each individual. As these algorithms target individuals, other algorithms are going to be needed to fight them.

As we segment people, they become numbers, and the biases within our algorithms are amplified. Policing becomes profiling. China has taken this policing to an extreme with cameras on every corner and facial profiling resulting in individuals being relocated to re-education centers. Every facet of human behavior becomes a data point, and this data will make sense to AI. The challenge is one of collecting personal data and protecting personal data.

Full Interview Transcript

Okay, how does the threat of microtargeting our forces: military, law enforcement, and political leaders, manifest over the next decade given an increasingly interconnected information environment?

That makes sense. Well, I would actually start with Foucault. He brought up Jeremy Bentham's panopticon. It's one of his most famous examples. It's a prison design from the late 18th century. And what it is, is it's a way of having - there's a person in the center who's the eye, who's viewing everything, and the prison goes around and circles around that person. And so, and all of the cells are designed so then every cell is visible from that center. So, what it lets the center do is turn a huge crowd into individuals and then handle them one by one because nobody knows whether or not they're being looked at. If they're being looked at, they'll be punished.

So, what we have right now is we're starting to get to the point where we can segment our society that way. We can pull out areas and target them and then there's a lot of practical risk in that.

But really what's happened is there's been a number of waves of change that have affected this over the course of the past um a couple hundred years. The main thing is during industrialization and the beginnings of bureaucratization in Europe and in Russia and other places. They, in order to manage these businesses, in order to manage cities, you had to produce data - you have to count things, you have to organize them, you have to label them, and you have to find ways and points of managing them. And so that pressure is building up toward the end of the 19th century. And it's a great Panic of 1873 with the crisis in the late 1800s like late 1890s.

You had waves of people moving into cities who are then unemployed and who become a difficult thing that you need to manage, right. So, there's a need for data everywhere and there's tons of data. The problem is so it's all in paper and files. By the time, jumping just a little bit ahead, but the Soviet system was built to suck data in and so you know after a

while of the Soviet rule in Russia, they had massive amounts of information. They had so much information they had no way of processing it. It was jammed up in the bureaucracy because they had no way of managing it. If you actually managed to report the telephone conversations of every CIA agent - I'm exaggerating - every CIA agent, it takes you a while to go through the log, right.

Unless - this is where we jump way forward - you start having processors, you start having the ability to externalize that processing and you start having artificial intelligence that's able to optimize itself to look for and to find patterns in that data. So, what you have is that panopticon. You have the ability to say, "Oh, hey, pick one thing right out of there," as opposed to generalizing, which is all you can do when you're when you're aggregating things and just taking in piles of stuff. So, I mean, that change obviously came about with the computer revolution.

So, I jump ahead. You know, wars. Wars throw gasoline [into] the fire of technology development particularly World War II. And so, coming out of that was the design of the computer. And [inaudible] during and um we've started to develop a different ability as humans that's making a big difference, I think, in the way that we're conceiving our history and our society going forward. And that is we are externalizing a mental process that we have not externalized before, which is processing - I'm not a neurologist, you know, maybe using correct terms - but we're externalizing the processing of information for the first time.

The last time we did something like that as a society of humans, as far as I can tell, is when writing was invented itself. The very beginnings of cities, you know, pretty quickly they had too many cows to count and so they started making marks and that started to develop the ability to offload memory, so you're actually offload[ing] storage and then over a long period of time managing that storage. Books, you know, the information all that kind of stuff, it keeps accumulating, right. But then all the processing, all of the actually thinking about the information, I'll be categorizing all the analysis, all that sort of stuff, is done by people until we're able to do that by computers. And now that we're able to do that by computers, all of a sudden, this whole vista has opened up and that's [inaudible] a hold of us, you know, the ability to microtarget people.

It can be, you know, we've seen things in the war in Ukraine, for example, where Ukrainian activists have found the Facebook accounts and stuff of the Russian soldiers and used us to track them and they've also gone and contacted their families and have said "Hey, do you realize what your son is up to in Ukraine? Because he's committing war crimes" - that kind of stuff - is its harassment that can affect the mental condition of truths. If you know that your family is being called, you know, called by the Ukrainians to harass them while



you're sitting there getting shot at, it's not good for you around, right.

So, there are all sorts of potential ways. The trick is again - and here's another way that this was used - is what Cambridge Analytica did in the 2016 election. They managed to use what Google and Facebook have started: this system, basically surveillance capitalism, accumulating information and then churning through that and having that data be basically the power of what it is that they do. Cambridge Analytica then, they worked with Facebook and came up with ways of - and again, I would have to put who's responsible for it. The point is that analysis was taking rather than using the usual analysis of voters and thinking about categories of voters and pointing at them and trimming messages to the best that you can with just the data ahead of you. What Cambridge Analytica did, and what Facebook has done, is allowing people to target different messages to different people so one candidate is not just one candidate. If there's a thousand people it can be a thousand different candidates, tailored designed to meet their expectations.

One person, you know, it's very clear through all the algorithms, pops up: they're extremely religious, that's been played. That one direction, you know, other things that they, you know, they like animals, they'll play that direction, you know, their entry points in.

I think there are future threats are going to be generated, a lot of them, are going to be generated by the algorithms that we put in. They're going to be machine generated and they may be things that we don't necessarily think of thinking about. The way machines think is different from the way humans think. And I'm not suggesting Terminator is right around the corner, but there are ways that, you know, that an algorithm can work in opposition to, I mean, the main thing is to say that we're going to need to use AI to predict AI. You have to fight fire with fire.

In that case, and there's this kind of, you know, and I think AI computers have demonstrated this in chess and other moves that they've made moves that grandmasters haven't thought, would never have occurred to them and now there's grandmaster chess players who are learning from the ways that machines played chess, right. They think differently than we do and so if we plan to outthink them, we're not going to, we have to work in connection with AI. There's no way around it at this point. And, you know, at its best it's an amplification of whatever it is that you of something good, you know, and it's worse. There's a lot of dangers, because it can target you and it can also create anytime you take a society or a group of people [inaudible] even and decide to how we're going to describe these people, get data on them.

We start to segment them. They start to become numbers, and when people start to become numbers, you can do things to them [inaudible]. The trick with a lot of these algorithms and a lot of the AI stuff is going to continue to be, is it appears because

it's a machine because, [inaudible] because the numbers are clear. It appears that that everything is simple and logical and straightforward. The problem is that those numbers come from someone, and the data comes from somewhere and that data comes from society. So, what you end up with when you start doing predictive policing algorithms. You end up with algorithms that amplify the racist policing that was there before, right. Because you're thinking about, "Okay, well how many? Where are all the crimes we're going to look at, all the crimes the crimes are there, because the police observe them." If the police are in another neighborhood, they aren't looking at other neighborhoods, right, so all the data that you're training that predictive algorithm on is skewed and it's going to focus again back on that place and give some negative feedback, right, so that that one neighborhood is going to be the prime neighborhood and it keeps getting pegged that way and amplified. So, those are the kinds of things that that can do.

I should jump onto one too is China. They are investing heavily in AI. It's a big push for them and we need to be concerned about that. They have a massive trove of data and not only have they created [a] functionally Orwellian state in Xinjiang in the western province Muslim leaders are put in internment camps and tracked all the time. Facial recognition on every corner of police and every section and things happen that they don't like the camera in your living room plastic box. People are taken to re-education centers; there's internment camps delivered.

Anyway, the point is China is taking every single one of everything a human being does is a data point and if you're trying to understand people you could throw all that stuff together and it actually will make sense to AI. And they're feeling data from everywhere, they're a data vacuum. They touch everything and they don't draw the lines that we do; we draw lines between private and public, and, you know, what who should touch what. But it's fine; they'll touch anything and grab anything. And so that means that their AI is going to be trained on data that we can't you know an amount of data and a kind of data that we don't have access to right.

And so probably one of the biggest things going forward is going to be to try to get their data, and it's going to be activities going after data sources that we don't have right now. And I would look at a threat to us as people coming into our data and we need to start thinking about that as a defense. You can't say you know oh well that's great Bank of America has got to go protect itself. No, you wouldn't say that if the, you know, an army was coming in to send fire to the Bank of America building you shouldn't say the same thing, you know, when it's a digital attack.

So, we need to start doing conceptualizing a little bit [of] what we expect out of them, of technology, and opening it up to the possibility that that you know it's going to kind of it's



going to do the momentum and we're going to have to tweak and poke to get things along.

James Giordano, PhD, MPhil, Professor in the Departments of Neurology and Biochemistry at Georgetown University Medical Center. Chief of the Neuroethics Studies Program, Scholar-in-Residence, leads the Sub-Program in Military Medical Ethics, and Co-director of the O'Neill-Pellegrino Program in Brain Science and Global Health Law and Policy in the Pellegrino Center for Clinical Bioethics. He is also Professor in the Departments of Neurology and Biochemistry at Georgetown University Medical Center.

Excerpt – Key Ideas

Targeting can be done both as a whole – targeting an entire subgroup – and by looking further within a subgroup to target individuals. Big Data is created by collecting a huge amount of data and metadata that can be used across a person's entire career. This data will be beneficial but can also be used to microtarget both individuals and groups after it has been collected and stacked, and then possibly hacked. It could be changed, and no longer represent reality. It can be used to find weak points in individuals or groups, and then acted upon within the community of interest.

Data on members of an organization will help understand the actions of those leading it. We will also be able to create synthetic biological pathogens to target individuals. As we look to safeguard and protect in the future, it will require:

- ▶ Identifying and creating awareness of issues
- ▶ Quantifying real threats and harms
- ▶ Mitigating contributory factors
- ▶ Prevention within society

This will be a competitive space. It is critical to maintain our ethics in the competition, as the totalitarian state is not a viable option – but it is for your competitor. They can make a strategic plan for the state, which is not practical for our society. They have a more seamless connection between government, intelligence, and commercial sectors.

Full Interview Transcript

BDJ: Question number one is how does the threat of micro targeting our forces, that could be military law enforcement or political leaders, manifest over the next decade giving an increasingly interconnected information environment?

JD: You know I think within the question they're really there are two subsections that are embedded. Number one is looking at forces on the whole in other words a mass effect

within the force whereby particular individuals or groups of individuals can be targeted utilizing the information that is available intramurally and intra-organizationally to others who are external to them.

The second part of the question is the idea of key individuals either intrinsic to those organizations or separately, for example politicians, policy makers, decision makers and various other forms of leaders whether they're political or charismatic or economic and how are those individuals viewed as high value targets and then targets of sort of high demand and high effect?

Let's take a look at the former and then move into the latter.

One of the key issues that's occurring right now, and it is a process in evolution and iteration is the use of big data and Big Data approaches so as to be able to force multiply capability and optimize performance within those organizations. Certainly, within the military; it's a lot of my own work. In terms of what types of data we need to be able to provide: metadata that can be then mined appropriately to be able to identify key variables, factors, and patterns that would be contributory to health, operational-occupational protection and enablement of the Warfighter, intelligence operator, and Personnel writ large across the board based upon specific characteristics both genetic characteristics as well as phenotypic characteristics that can then be fitted into a larger schemata of bio-, psycho-, social-, economic- profiling in a non-derogatory way to establish both agnostic patterns, in other words we go in not looking for a particular pattern, but the pattern is then generative, or looking for key patterns, in other words an agnostic approach that then identifies those patterns and allows us to then target those patterns as means for sustaining, maintaining, or in some cases implementing key performance variables in those individuals across their career lifespan - their career span.

So in other words, we're utilizing these multi-fold, multi-dimensional, multi-domain data in those ways that have an identifiable positive effect intra-institutionally and organizationally and in some cases inter-organization - some of the work, for example, that's being conjoined by title 10 and title 50 assets, for example, are seeking to try to bring those two communities together so as to be able to manifest a better idea of who are key candidates for particular performance type jobs. What are various stressors? What are various resilience and resistance factors that may in some way prevent mitigate or, at very least, rightwardly shift the onset of denigrative factors that would then compromise these individuals' capability both again as individuals as agent actors and within particular groups of teams?

So, the idea of utilizing multi-fold biopsychosocial plus data for organizational operationalization and enhancement, enablement, and capability is becoming the ever-

new norm. Granted, along with that, come a host of concerns as well as postures about the relative security and stability of those data provenance, custodianship, and downrange, what is being done with those data and how are those activities with those data going to manifest with regard to personal concerns, professional concerns, and concerns with regard to individual, public, and national security on a larger scale?

The problem is that those things that are being used intra-institutionally and organizationally may also be assessable and accessible externally through a variety of different means. Some of those means intrinsic to the electronic hardware used to store and transmit those data. But more and more the idea that the nature of these data requires data nodes that, while are secure, must interact along edges to create networks for real-time acquisition, assimilation, and synthesis, and provenance and use of these data in relatively real time. So, in other words, these data need to be stacked or at least the, if you will, utility nodes of these data need to be stacked within rapidly flexible, modifiable, and adaptable networks.

Well, what one of the old adages here is that those things that are stackable may in fact be hackable - not at the nodes themselves, but on the transfer aspect of data, because many of those internodal mechanisms and processes, and actually machinery functionality-hardened software may have provenances external to the organization that may be somewhat ambiguous, or in other cases, a cult. And as a consequence, access to those data then allows their relative usability across a range of potential capricious, if not nefarious, implications and possibilities.

So, for example, utilizing individuals' data, or group data, can manifest essentially three security, stability, and therefore, long term, if you will, national defense implications. First, is that the data themselves can be purloined - changed. Data are information. Information represents knowledge. That knowledge is taken to be sacrosanct for reality. As a consequence, we regard and respond to data. And if the data tell us A, B, and C versus X, Y, and Z, then we will regard and act upon A, B, and C that we believe is veridical, and as a consequence, certain decisions and consequential actions of those individuals or groups of individuals are regarded and treated.

Point number two. Those data are also representative of facts. Facts that range from the cellular all the way to the social, from the molecular to the mass effect, and from the individual to the institutional if not international. Because you go up to their range of what those data represent, and therefore, what they articulate. Each and all of those data taken individually and then taken in mass can also be used to develop precision engagements. In other words, the more I know about you the more I'm able to elucidate various vulnerabilities, weak points, if you will, that are loci for targetability. The more I know about

you the more I can target your weak points, simply put.

Third, is some combination of those two. So, now what I'm doing is I'm utilizing those data to create apparent weak points, vulnerable points, volatility points, that are then acted upon or responded to within that community of interest. In other words, if what I'm doing is I'm looking at these data - manipulating these data - and from the manipulation of these data creating what looks like vulnerability or vulnerability [sic] aspects. The organizations themselves will regard those data as realistic and very often will act upon them. I can create trends in various organizations and institutions that realistically are then responded to either by those organizations or institutions directly internally, or externally by those organizations, audiences, and polis, that they lead they affect they engage, etc.

These three domains are not mutually exclusive. We certainly have the capability for data access, data hacking, data purloinability, [and] manipulation. We certainly have the capability to take those data and utilize those data together with extant techniques and technology such as machine learning and various forms of artificial intelligence, to develop, if you will, precision pathologies - some that are biological - others that are far more psychological and social. The pathological nature is exactly that it creates a disruptive effect in one or more domains of an individual or interpersonal or inter-individual system that then manifests itself and then causes some dysfunction, disorder, etc.

And then, of course, the third represents the viability of accessing those data, creating upsets in the data, and as a consequence propagating misinformation in and around community of share and stakeholders of effect.

BDJ: Thank you for that, sir. You've already touched on this, and I just wanted to tease this out a little bit more. When you think of any, what are specific threats to national security because of this adversary's ability to mine these oceans of data, as you've just talked, about identify and affect individuals at scale to achieve the adversary's objectives?

JD: Let's take a look at two. Let's take a look at a large scale; let's take a look at a small scale, selective high value target and the disruptive or rippling effects that occur downstream.

First, if I'm able to access individual data and multiple individuals' data within an institution or organization, I have insight to a variety of different levels of that organization's functionality. In other words, I know what makes these people tick. I know where their vulnerabilities lie, [their] volatilities lie. I can also use those data in ways that are not only definitive and descriptive, but in some ways may be predictive. And, as such, I may be able to manipulate those data to change descriptivity, definitivity, and perhaps even alter the trajectory of how those individuals are regarded and treated within and beyond those

organizations. Point number one.

The second point is something that we're very concerned about which is primarily on the biological side is that we have the capability right now to be far more facile in utilizing synthetic biology coupled with certain genetic and molecular techniques to be able to develop true precision biopathologies. Whether those pathologies are variant microbial organisms - viruses, bacteria, novel fungi - to be able to create various proteins and anomalous protein folding that can then be used to target specific individuals based upon their biological and in fact immunological vulnerability and susceptibility. We have the capability of doing that. And if we know where these individuals are situated within the larger social fabric based upon their social data, their demographic data, we can then utilize those data to identify who those key targets are and their relative value and the effects that their value will incur within the organization and beyond - and target them and target them in three ways.

Number one, target them in ways that are overt and explicit. Number two, target them in ways that are either clandestine or covert. [Three] And through either of those two, incur effects it could be either acute and more tactically viable, or very often, strategically latent, so that then the effects become manifest over time and realistically the footprint of data manipulation or database manipulation of some biological host set of variables, is far more difficult to identify and therefore to attribute.

So, this represents if you will, the problem space. In the latter condition, where we're looking at key individuals - let's say a political leader, a military leader, a charismatic social leader, an economic leader. Same thing here. If what we're able to do is manipulate that individual's historical personal data and those data are then made available, it can in some way purloin that individual's reputation, that individual's regard among their followers, and/or the way those followers then respond or react to that individual and that individual's presence, capability, etc.

Secondly, if we can identify key variables of that individual and those variables can then be accessed and affected, we can then target that individual biologically, psychologically, sociologically, and economically in those ways that will affect their literal political value - in other words, their value with their attendant polis of followers who would then be the audience of influence. So, by affecting the individual who is a high value individual - either biologically or by manipulating their data so that reputationally by virtue of their regard, visibility, perspective, within their response of polis - we can then get these ripple effects that are at least disruptive and, in many cases, can be destructive, because they are destroying the status quo and creating opportunities for vectoral insertion of other influence factors. Over.

BDJ: That's excellent, sir. And then, so, finally, as you look 10 years out how will all of this, what you've described, how will this potentially affect our ability to conduct our missions to defend the nation, protect U.S. leadership, and safeguard the U.S. economy?

JD: I think that the question is profound because it really involves a multi-fold approach. The multi-fold approach that we've advocated is a four thrust approach and those four thrusts are not mutually exclusive - they are indeed interrelated. And coming from that interrelatedness also speaks to the need of conjoinment of resources, services, and personnel on a broader scale which I'll speak to momentarily.

To describe the four-fold approach. In short, the first thrust involves identification and awareness of the issues; realistic assessment of the relative burdens, risks, threats, and potential and realistic probabilistic harms that those threats would incur. Not all risks are threats; not all threats are harms. And it's going to become important with regard to resource allocation, appropriation, and conservation and efficiency of force to be able to not only qualify and identify what those burdens, risks, threats, and harms are but to create some type of threat modeling and threat indicators that are quantitative so as to be able to recognize which burdens to risks, to threats, to harms become more quantitatively probabilistic and therefore, would engender the focus of resources in terms of things like surveillance, preparation, responsibility, and reaction. So, that second phase is quantification of real threat and real harms.

Third phase and third thrust is actual mitigation of those factors that are contributory or at very, very least manifest and effective in establishing those burdens, risks, threats, and harms, and doing so in a way that is once again quantitatively and probabilistically inferential and influential. Let me explain. If we can determine that a particular factor - let's call that factor X - has some fairly high probability of inducing some downrange vulnerability or impact variable - impact manifest, sort of rippling effects - well, then clearly, the use of our resources to be able to mitigate X on a variety of levels - either at its source and/or in range of its actual affected substrates and variables - is somewhat higher than another variable which we could call variable Alpha. So, the qualification [and] quantification becomes very, very important to the net third thrust which is mitigation - mitigation appropriately - so as to be able to identify what are maximal threats, risks, and harms, and those which are, for example, sub-maximals both temporally, in other words, what is the low-hanging temporal fruit - this could happen right away - as well as influentially. Yes, this might not happen right away, but if we let it evolve to a particular point the impact or manifested effects of that thing are going to be far more devastating, far more widespread, etc.

The last thrust is prevention. And prevention is a little more difficult. But one of the

ways to prevent these types of things is by exploiting peer competitor whom adversarial capabilities - inclusive of exploring certain aspects of their strengths so as to then utilize those strengths to be able to render particular weaknesses. Now, that's a mouthful and I understand that. And there are a couple of ways to do this. One is to understand those areas where potential competitors and adversaries have true viability and strength in those dimensions that we are not either capable or willing of engendering, entailing, or obtaining. A number of factors that go into that. Certain ethical issues - ethical issues that arise from culture, policy, and legal issues, international law issues - what things are protected by international property rights and that may be commercially veiled, that as a consequence, we may not necessarily be able to change but we can certainly identify.

Along with that is the idea that recognizing there is going to be this competitive space - this competitive thrust - is to create certain co-dependencies in the escalation of those competitions. This is sometimes referred to as co-op competition - cooperative competition. We recognize the competitive aspect is there, but what we then do is we develop, insert, and fortify those areas by which some level of cooperation is required so as to be able to then induce those dependencies that will gate, meter, and govern, to some extent, the range and the impact of those effects of those competitive interactions.

So, in other words, what we're saying here is, yeah, I know you're going to succeed in particular areas, and we don't necessarily have the hutzpah, [or] want to change our moral and ethical fabrics so as to be able to do the things you're going to do, but we also will recognize that if you do those things you're going to need these factors. And these factors are things that we can control. And in controlling them we will be gating or governing how it is you're able to manifest whatever levels of hegemony you may then seek to acquire. It's all about differential purchase. It's all about acquiring domains of purchase, leverage, and ultimately controlling hegemony. What should be, I think, intrinsic or perhaps derivative to that type of a statement, is the implication that readiness and preparedness is not assuming that we are the only superpower.

I think it becomes very important to recognize that given a host of factors - some of those factors cultural, social, economic, and certainly based upon political structures that differ from open liberal democracy such as we have here in America and among many of our international, economic, and military allies - that "capabilizes" other systems, to be able to do certain things that might be difficult, somewhat more time consuming, or, in other cases, not tenable for us.

I'm not in any way advocating that we change our political system into its structure nor am I advocating those things that we see, for example, in closed democracies or in totalitarian states - not at all. What I'm saying, is it becomes important to recognize what those

regimes, their structures, and functions enable and empower them to do, so as to be able to effectively develop counters and those counters need to be contingent upon what are the relative dependencies that those programs, those products, and those deliverables and their effects require and then exploit them.

The other thing that is, I think, important to understand is that even if we consider ourselves to be one of many superpowers, there is something of a disadvantage that is intrinsic to our political system. And I'm not advocating changing the system. But what I am advocating is the addition to that system. Namely, a perdurable strategic plan.

One of the things that our peer competitors has is in fact a viable multi-year plan that orients to longer-range tactical benefits and capabilities towards strategically latent effects with specific goals of strategically latent hegemony at a given point in the future. And what our adversaries and peer competitors tend to do is to work deductively in other words if this is what we're looking to achieve at point X in time, what is going to be necessary to manifest within global ecologies of power, of sociology, of capability so as to begin to fertilize, manifest, and then guide, vector, "trajectorize" our capability to meet that goal as established at that timeline? What that dictates is a keel, to utilize nautical terms, of a strategic plan. That irrespective of which way the wind blows orients the relative stability of, if you will, the ship upon which you are sailing. But you don't want to have happen is to have that be imbalanced in such a way that the sails dip and the sails come down.

One of the problems we have is that in the United States there is no overall strategic plan other than an ambiguous statement of defending the Constitution against all enemies foreign and domestic. The Lord knows I took that oath. What does it mean in terms of large-scale liability within the multiple organizations and institutions that constitute our governmental resource power? Well, it means very little if every four to eight years the entirety of the political system changes and with each incoming system there is a relative reorientation to what is prioritized.

I recognize all of the issues, variables, and contingencies that go along with partisan divide and partisan replacement that occurs as balances of power within our political system every so often. But what should be entertained should be appreciated and apprehended is that our near-peer competitors could [become] potential near-term adversaries in the next 10 years, do not have that ambiguity, do not have that level of, if you will, lassitude that occurs every four to eight years with the re-establishment of what might be tactical orientations and plans. Instead, they are adherent to a strategic plan relatively irrespective of whatever the local and short-term power dynamics are within their government.

Point one.

Point two. [Our] most predominant trans-Pacific and trans-Atlantic near-peer competitors – potential adversaries – have a relatively seamless triple helix of government inclusive of military intelligence organizations, large-scale research organizations, and the commercial sector. That allows relative direction, cooperation, the absence of the need to define what is single- or dual-use, as well as the capacity of commercialization in the large-scale production under a commercial veil of intellectual property, that essentially enables them to create large-scale multiple thrust activities utilizing a triple helix whole of nation approach. Not just the whole of government. My previous point about governmental cooperation, integration, and adherence with a strategic plan that is implemented in and across five-to-ten-year intervals of tactical orientation, is not just a question of whole of government - which requires a cooperative effect, without doubt.

Again, I'm not about to deny the reality of certain partisan divides. Irrespective of those divides what must be held in common is your strategic plan towards the overall benefit of the nation irrespective of its partisan governmental orientation. Locally, regionally, there must be that national interest with regard to national security and defense - as it exists on the reality of the 21st century global stage - and the capacities that science and technology afford for these levels of infiltrations and disruptions. That requires a whole of nation approach where the resources of multiple dimensions of the nation governmental coordination and cooperation, private institutional coordination and cooperation, large-scale commercial and industrial coordination and cooperation - work within that larger triple helical orientation on those issues that are of key import to national security, intelligence, and defense, inclusive here of bio-cyber security. Over.

John Hammond, *Cybersecurity Researcher, Educator, and Content Creator*. As part of the Threat Operations team at Huntress, John spends his days analyzing malware and making hackers earn their access with the same tradecraft learned and used in Capture the Flag training, bug bounty, and penetration tests.

Excerpt – Key Ideas

The value of data privacy and information in our networked world is increasing. Social engineering, for example, is critical to spreading malware. The impersonation of individuals you may have never met but might have a reason to collaborate with has traditionally been an attack vector. One of the latest scams is advertising the ability to improve your social media presence through downloading and running an app which harvests credentials and session tokens for later exploitation. Deepfakes are another useful tool for social engineering, as well as spreading disinformation and damaging individuals' reputations.

Full Interview Transcript

Hi everyone. My name is John Hammond. I'm a senior security researcher at a company called Huntress and for our time together I want to tell you two different stories focusing in on microtargeting and the value of our own data privacy and information, and how that can be at risk or endangered in some ways in the growing, interconnected world that we live in.

So, first things first. To kick it off I'd love to do a little bit of show and tell. So, I am going to share my screen. I wanted to tell the story from a recent case, a recent incident, a recent investigation that I had done with the team of my own that was tracking some specific targeted incidents. There is an individual that is at the top of some organization - uh for the sake of confidentiality and sharing the story, we've redacted all a lot of those details - but ultimately, this organization is a national think tank. They're doing research on foreign adversaries and other locations across the world that might have of some specific power and prowess in weapons arms nuclear techniques and things that we should kind of be concerned about.

So, ultimately, we're digging into malware, we're digging into cybercrime, and what threat actors and adversaries might be thrown at this organization or any others to do their own information espionage to see what they can do to listen in on that environment. There's a lot of really neat stuff as to how a threat actor might have gained access. Ultimately, it digs into phishing email - "Hey! That's classic social engineering and deception." I won't bore you with too much of the nitty-gritty details and all that nerdy stuff, but I think it's super-duper interesting that the malware string that they used specifically had embedded in its code references to this individual user - that person, that human being, that they were targeting - that they were stalking on social media. That they were looking all around to ensure that the malware that they would detonate the threat against them in the organization was specifically aiming at that one individual. It's a wild story.

If we were digging through this looking only at how can we do some sort of - trying to get the right word here - "blast radius" of other individuals inside of that environment but ultimately reach the specific target - again I don't mean to get too far into the nitty-gritty - but, we were able to dig through these specific phishing emails that fooled this user. It's wild to see a threat actor posing as a reporter - someone from Voice of America. Dealing with the sort of charade and facade that they're doing a report and would like some information as part of an interview or whatever that user is willing to share.

They go back and forth, and this user builds up trust [with the] threat actor without immediately asking for them to "Hey, look at my document and explore this file that I'm sending to you in a malicious attachment." But they build up some repertoire and

eventually include a link that detonates a malware. Kind of wild; kind of crazy. Interesting to see the others that might be present in that chain. But turns out this became a story and it's been a recent coverage. There's actually been a "Hey, threat actors and hackers using these personas, these individuals, that they might impersonate to trick other researchers to share information or ultimately implant a back door and something to listen in and steal all of the information that they might be collecting even on those other adversaries." Yeah, cool.

The other last tidbit that I'd love to give you a little bit of insight on - I know we don't have a ton of time - but there was a super interesting scam that I saw floating around on the internet - over on Facebook. Massive social media website where all of us tend to willingly put our own information out to the public. And there were comments that were suggesting hey if you wanted to get new likes, if you wanted to improve your profile page presence, if you wanted to network with new people, you could use this tool - you could download and run this software. It would, of course, need your own Facebook credentials to be able to network and connect with other people or gain lots of new likes on your page, but you can expect hey, that utility would end up stealing and grabbing all those credentials and collecting those passwords to gain access to that session token for later harvesting, to do more malicious activity or just spread and gather new information.

It's wild to see all the information that you might put on Facebook, like other birthday information, relationship status, pictures, and other things will then just be piled up and then collected by a threat actor to do something more with. Crazy to see that exists.

But I wanted to give that idea to you, and I wanted to reflect on that just a little bit more because whether we're looking at microtargeting one specific individual, that might be in a place of power or casting a wide net for anyone Joe Schmoie down the street made by myself or any others. What is the information that we put out there and how easily can we give that to threat actors to profile us, when adversaries are now in the age of artificial intelligence or machine learning?

I think one specific spooky thing is deep fakes. Hey, you've collected enough information even on me. In this video you could replicate my face, my voice, and then masquerade as me or anyone else in some other online presence or campaign.

It's wild to see misinformation could grow at an alarming rate. And I think for the future that's not going away. We're going to see more of it and it's hard to get off this treadmill, but I think the best thing we can do to fight - that is, awareness, education, and keeping folks in the know that this stuff is out there. It really exists. And each and every one of us is susceptible to it.

When we're thinking about security - when we're thinking about our own personal security or national security - it's our responsibility, it's everyone's responsibility, and the onus is on us. And I hope that is some at least interesting food for thought and some parting wisdom for us to think on.

Dr. Lydia Kostopoulos, *Strategy and Innovation Advisor*. She speaks and writes about disruptive technology convergence, innovation, tech ethics, and national security. In efforts to raise awareness on AI and ethics, Lydia makes reflectional art #ArtAboutAI. She also made a game about emerging technology and ethics called *Sapien 2.0*.

Excerpt – Key Ideas

Communication and technological advancements are changing society and the future of financial cybercrime. The future of finance (e.g., a national cyber-currency) will change the nature of financial crime [as one type of microtargeting risk] as the architecture changes, including efforts to bypass the international system. The existence of these currency architectures in cyberspace offers an increasing attack surface and the potential for cyberattacks to influence the operation of the global financial system.

In addition to this, the ways individuals authenticate themselves and purchase goods are also changing as more of the financial industry shifts from paper- to virtual transactions, and as smartphones are used for payments and to authenticate identity. Identity fraud will become increasingly complex as social media profiles and implanted devices are used to pay for goods and services in the near-future.

Full Interview Transcript

The question at hand is what will future cyber-enabled financial crime perpetuated by either cyber criminals or nation states look like 10 years from now. But before answering that question, I think that it's important to reflect on where we are today in the financial world. Today, we have constant cyber tax against banks against multifactor authentication on banking apps. And this is just the beginning of it. The core infrastructure of the financial industry is also being threatened by attacks on swift. This has really great implications, the international financial infrastructure, as we look to see what kind of future cybercrime, we would have in the financial sector 10 years from now, we need to also understand where we are in terms of our industrial revolution. Right now, we're in the fourth industrial revolution. One that is characterized by IOT – internet of things – fast internet, 5g, AI, quantum, all of these technologies are changing the paradigm in which we operate across every single industry.

And because of that, we also need to rethink not just the way we do transportation, the

way that we do medicine, but also the way that we do finance, the way that we exchange goods 10 years from now, we can imagine that we will see different forms of currencies, so cryptocurrencies, stable coins, but also state backed digital currencies. These will be very important in having a backup to the fiat currencies of today and that infrastructure right now that we do use today, that is threatened. So, what will the future of cyber enabled financial crime look like 10 years from now? The ideas I have are as follows one cryptocurrencies and stable coins, as these become more popular and used in conjunction with visa credit and fiat currencies. This will be a type of finance that will be lucrative to steal by different cybercriminal organizations.

Similarly, there are rogue nations who will seek to use cryptocurrency even more so that they can bypass the international system. This already exists today. But they will be able, they will be using this more and, and more in 10 years from now two looking at the fiat currencies, we talked about earlier, how right now the financial infrastructure we have today can be threatened quite severely by cyberattacks. And there is a need to go digital. There are nation states right now that are already looking into a digital coin or a digital currency that would be state-backed. So, a national currency right now China's already experimenting with that as are other countries, 10 years from now, this will be a source of competition between nation states, but also an area where one nation could commit financial war against another nation by attempting to digitally attack or undermine the cyber currency of a different nation that is backed by a different nation.

Three. The ways that we are going to be authenticating ourselves to pay are going to be very different 10 years from now, we're going to be using biometrics our face, our eyes, our fingerprints, but also we'll be using our mobile phones with different social media profiles that we can use to pay or other authentication methods that are internationally accepted, such as, for example, Apple Pay or Google Pay. And if, and when these organizations decide to create their own digital currency or own form of credit, this will really change the paradigm in which monetary goods are exchanged, but from a cybercrime perspective, stealing profiles will be very lucrative in this sense. Identity fraud will become much more serious when we start to use our bodies and our social media profiles or any kind of digital profile to pay for goods and services. The future is definitely hard to predict, especially in this current environment, but I hope these thoughts could be abuse as you explore the potential threats in the financial cyber-Naval crime space. Thank you.

Peter W. Singer, *Strategist and Senior Fellow at New America*. He has been named by the Smithsonian as one of the nation's 100 leading innovators, by Defense News as one of the 100 most influential people in defense issues, by Foreign Policy to their Top 100 Global

Thinkers List, and as an official “Mad Scientist” for the U.S. Army’s Training and Doctrine Command.

Excerpt – Key Ideas

We typically look to the past to grade our visions of the future. Our mistakes are not based in missing [Nicholas Nassim] Taleb’s black swan, but in failing to identify the “grey rhino” – an idea or trend that is clearly evident, but not easy to talk about. The trends looming in the room with us today that will change technology and security include AI, robotics, and their influence across society, especially all aspects of the economy. There are military aspects to these technologies as well, as they will help make decisions from logistics to medicine. The key to all these technologies is the network:

- ▶ The weaponization of social media
- ▶ Deepfakes blurring the line between truth and fiction
- ▶ Using the Internet of Things to control the physical world

There is a dual nature of trust involved in all these things – trust in people to be truthful, and trust in technology to perform the intended outcome. This has implications for multi-domain operations all the way down to individual battlefield actions, including the potential for tools and technologies to be delegated tasks as a wingman or partner. We will need to change how we visualize and train – to explore and implement these emerging technologies rather than simply validate them. And in addition to training, we need to watch current conflicts carefully to identify battlefield successes.

Visualizing and communicating these ideas is another challenge to overcome. We must get these ideas into the minds of the professionals who will implement them. “Useful fiction” is one technique, bringing latest ideas together in narrative form to make them more digestible. These stories and conversations must include the evaluation of sacred cows and the elements that need to change that are nonetheless hard to talk about.

Full Interview Transcript

I’m someone who wrestles with the future. And there’s a challenge in that. There’s a belief that it is something that is impossible to predict. Indeed, a senior U.S. defense leader described how trying to project the future was like driving in the dark with your headlights off as if that’s, you know, something you ought not to do.

But there’s an interesting pattern that happens when we look not towards the future, but rather towards the past. And when we’ve gotten the future incorrect - consistently, the failure is not from a so-called black Swan, some kind of unimaginable, rather it is repeatedly what you might think of as a gray rhino, a trend, a topic that was fairly obvious. It was just uncomfortable to look at, to directly stare at, to admit that it was in the room



with us. So, when it comes to the topic that I've been asked to speak to you about technology and security issues, what is it that lies in front of us?

I think the trends are fairly clear. Here again, obvious. It's the leap of game changing technologies that are playing out over the next decade plus. It's the realm of artificial intelligence, where we are seeing breakthroughs in a technology that is something that we've talked about for literally millennia. You can find discussions of artificial intelligence and everything from ancient Greek mythology to old Judaic text. Maybe you're a science fiction person. Well, over a century, we've been talking about this moment when AI becomes real. It's not just the software side of AI. It's also about the hardware side of robotics and how we see it playing out in all sorts of shapes, forms, roles, users. But again, don't just think about this as a technology that might be out there in the field and playing out in terms of security. It's also how it affects the broader economy, society writ large. For example, Oxford University did a study of 702 different occupational specialties and found that roughly 47% of them are at risk for complete replacement, reduction, or drastic redefinition over the course of our lifetime.

Now each of these areas have their military parallels. Again, so the issue with robotics is not the so-called lethal autonomous weapons system, killer robots, or nuclear weapons being controlled by AI. It's about how AI covers the entire spectrum and everything from decision helping to military medicine, to logistics you name it. It's also another kind of change, not just in terms of the software and the hardware, but what binds it together in terms of the network. We see this playing out in a couple of key ways. One is in the weaponization of social media where you've seen it affect everything from, politics to public health, to battlefield behavior or to mass killings going after hundreds of thousands of people. This area is going to get even more challenging because of going back to one of those prior topics, artificial intelligence, where the line between what is real and what it is not, is very tough to figure out now and be even more so as we blend in greater levels of AI – what is properly known as deep fakes.

But there's a second key change in terms of the network. It's the shift of the internet from being about merely communication, which was game changing enough to the concept of the internet of things. It's an idea that originates in 1999 and is becoming real now - where we are using the network to control the operations of everything from smart cars, smart power grids, thermostats to the individual parts of systems. Now that will open up huge possibilities over \$11 trillion in value, but it'll also open up new risks. It doesn't just drastically grow the attack surface of what you might go after. It also changes the kind of effect that you might have with digital attack, where you're not stealing information or spreading information, even if it's false. In this case, you are causing kinetic change in the world, physical damage.

We're also seeing a whole change in terms of the very approach of computing itself. When you think about quantum, and this is from a project that we are doing with NATO ACT, where we will see the ripple effect of quantum in everything from computing, communication, encryption changes, to sensors. My point in this is that if you pull back and think about it, we have a massive rethink of not just technology and its possibilities and perils, but also what it means for security in the battlefield itself. Now that is very bold to say, but again, look back in history. Why should we think these changes in everything from AI to robotics to quantum are somehow going to be less in their effect than say the machine gun in 1914 or the tank and the airplane in 1939. And in fact, shouldn't they be something more because we're talking about a technology that unlike ever before is always improving, ever more intelligent, ever more autonomous. And so that we think I believe should go beyond what we see before.

So, what can we do about it? Well, I would argue there's a series of measures that we need to undertake. One is education and awareness is now a core task of leadership. For example, the case of AI, 91% of leaders say AI is the most important game changing technology that's out there. 17% - though - say they understand AI, how it works, what are its ramifications and its dilemmas. That is a massive delta between what you think is going to be important and how well you understand it. And it's not just specific to AI it's any of these new areas. It's not just looking at yourself, it's looking at your organization and saying, not just what is important, but how well do we understand it?

Second, every aspect of this is not just a story of technology. It's a story of people. And so if we're looking at how we handle talent management, all the human questions, everything from recruiting to assessment, are we making changes that are equivalent to these other changes that are going on out there? And if not, why would we expect the human side to keep pace?

Another part of this is, is the key issue of trust in all of this, but it's the dual meaning of trust. You can think of trust as a kind of emotional state: "I trust you". But it also has a definition in terms of how engineers might think of it. Does it behave in an expected manner? Does it meet the way that we understand the world? So, think about it this way. You can trust someone, but you can also trust that someone is a liar, and you know that they're always going to lie to you. And so, with that expectation, you can operate effectively in the world. And so, these two meanings of trust are the key to not just integrating the technology and using it to its full effect. But also, these two meanings of trust are how any adversary is going to go after us.

Another part of this in terms of these dual issues of trust, but also larger sweep of change - is how it will affect what we're thinking of as multi domain operations and the task of multi domain integration. Essentially this is going to affect not just overall security, but



individual battlefield behavior. And when you get inside this, it also means it cuts to the heart of the new concepts and doctrines that we need out there. What is our vision of the technology and our relationship with it in terms of everything from trust to the uses that we make of it. So, for example, is it a tool that we are using or is that technology not just merely a tool, but it is something equivalent to a teammate, a partner, a part of the organization, a wingman or no, it's beyond the equivalent of a tool or a partner. It is an autonomous agent that we delegate out there. And not just that we delegate it out there in a single, but also maybe we delegate it out there in terms of a massive number. How we answer that is again, key to the future, whether we're talking about the future of cyber war, air warfare, you name it or how they come together.

But it also means that we need to undertake another kind of change. We need to change how we visualize and train for the future, too much of how we approach it right now is validation: validating, existing concepts, existing technologies, or validating our existing relationships, the kind of exercises that we love to do. We're allies, let's go out there together and show how much we like each other, which definitely have value, but we also need to do more of the, the kind of exercises that we saw back in the 1920s and 30s, whether you're thinking of the British experimental mechanized force or the American Army Louisiana maneuvers, where the goal was not just to figure out the difference between horses and mechanization, but how is this technology best used in everything from the technologies to the tactics. But the big lesson from that period is again, it's about the people figuring out who's thriving, what kind of training matters most. And then the most important lesson is not just learning the lesson, but how do you actually implement them after the exercise? Because sometimes they get implemented and a lot of times they don't. As part of this, you should also be seeking out lessons in terms of what works, what doesn't - before you actually commit.

This is an example from U.S. Navy exercises in the 1920s, where they wanted to learn about the new concept of an aircraft carrier. There were two different approaches to it that you can see here. The USS Paducah on the left because it was the aircraft carrier was for blimps. And the USS Langley on the right, the aircraft carrier was for planes. Now compare that where they actually went out there and wrestled with it, to how we would do it today, where we already commit to not just the concept, but entire ship classes before we've actually figured out what works or not. Better to learn during experiment then later on in a war. You also want to learn from other people's wars. So, you go back in history, and you look at the example of the Spanish civil war, the insight that it provided to what would happen during the blitzkrieg.

So, what about those other nations' wars out there today? Everything from what's happening in Libya to Ukraine, to, as you see on the right, the war between Azerbaijan and

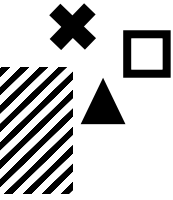
Armenia, where through very skillful use of bringing together electronics, cyber, unmanned warfare, the kinetic side, the Azeris were able to take out at least according to open-source intelligence, 46% of Armenian armored vehicles and 93% of their artillery missile systems in just a matter of weeks. That kind of change is important, not just for that conflict, but what it means for all the other future conflicts out there.

We also need to change, as I mentioned, the way that we visualize and communicate. There are more effective manners than producing white papers that people don't want to read, or they don't digest the insights from it. We've been using a practice that we call useful fiction that brings together non-fiction analysis and research with the oldest communication technology of all – story. You can think of useful fiction in a different way is being akin to a morning smoothie. Where you've got science fiction on one side (techno thrillers). They're like a milkshake - they're entertaining, they're tasty, they're fun. At the other end of the spectrum, you've got the vitamins, kale, something that's good for you. That's that research, that's that strategy paper. What useful fiction is, is it's like a morning smoothie. It takes the kale, the vitamins of the insight, but wraps it within a tasty package. An example of the potential of this is a project we did with the Australian military, where they had a 21-page report on defense education enterprise reform to deal with some of these new issues that we've been talking about. It's a great report, but it wasn't striking with a desired effect. So, we worked with them. We took the three key themes, the 37 key insights of that report and turned it into a narrative and a piece of art called "An Eye for a Storm." In terms of the impact of it, it's been read by over 12,000 readers, all the way up to the head of the entire Australian military and six current or recently retired U.S. four stars. By bringing in narrative, we were able to reach an audience that a typical white paper would not be able to. And if you can do it on defense education enterprise reform, you can do it on any topic, including that of WMD.

Finally, we need to kill our sacred cows. What is the equivalent to the battleship in 1941 or the horse cavalry in the 1930s? What is that technology that it's not ready for the future war, it's probably not ready for the present war. But it's again, not just about the technology. What are those organizational structures that were developed for the past but aren't appropriate to the present and future. And you can identify sacred cows by not just what's inappropriate, but what is it hard for us to talk about out loud?

And so, with that, I know I've thrown a lot at you in a limited amount of time. I would leave you with just one key takeaway, given all of the change that's going on out there around us, whether it's technology, security, politics, society, given all of that change – nations, organizations, individuals that look at that change and decide to stay still, will be choosing to lose the future through their inaction. And I hope none of us do that. Thank you.





APPENDIX C

Bibliography to “Engineering Consent: An Early 20th Century Guide to Manipulating the Masses”

- Bernays, Edward. “Emergence of the Public Relations Counsel: Principles and Recollections,” cited from *The Edward Bernays Reader* (1971) by Edward Bernays, Ig Publishing (2021).
- Bernays, Edward. “Manipulating Public Opinion: The Why and The How,” cited from *The Edward Bernays Reader* (1928) by Edward Bernays, Ig Publishing (2021).
- Bernays, Edward. “Propaganda,” cited from *The Edward Bernays Reader* (1928) by Edward Bernays, Ig Publishing (2021).
- Bernays, Edward. “*The Engineering of Consent*” (1947), cited from *The Edward Bernays Reader* by Edward Bernays, Ig Publishing (2021).
- Brandt, Allan M. “Engineering Consumer Confidence in the Twentieth Century,” cited from *Smoke: A Global History of Smoking* by Sander L. Gilman and Zhou Xun, eds. Reaktion Books, 2004.
- Brandt, Allan M. *The Cigarette Century: The Rise, Fall, and Deadly Persistence of the Product That Defined America*. Basic Books, 2009.
- Cohen, Lizabeth. *A Consumer’s Republic: The Politics of Mass Consumption in Postwar America*. Vintage Books, 2003.
- Kluger, Richard. *Ashes to Ashes: America’s Hundred-Year Cigarette War, the Public Health, and the Unabashed Triumph of Philip Morris*. Vintage Books, 1997.
- Lippman, Walter. *Public Opinion*. 2012 Martino Publishing reprint of 1922 original.
- Tye, Larry. *The Father of Spin: Edward L. Bernays and the Birth of Public Relations*. Henry Holt, 1998.
- Welshman, John. “Smoking, Science and Medicine” from *Smoke: A Global History of Smoking* by Sander L. Gilman and Zhou Xun, eds. Reaktion Books, 2004.



