The MIROR JOURNAL

Managing Insider Risk and Organizational Resilience

IN THIS ISSUE

Mission First, People Always:

Three Ways to Elevate Your Insider Threat Program Using Protective Intelligence

The New Insider Threat:
How Commercially Available Data can be used to Target and Persuade

Stolen Valor:
Use of Military Narratives in White Supremacist Chatrooms on Telegram

Volume 2 | Number 1 | Summer 2024

WEST POINT PRESS

The Department of Defense Insider Threat Program

The Department of Defense (DoD) Insider Threat Program leads DoD efforts to prevent, deter, detect, and mitigate insider threats to the DoD enterprise.

Located within the Office of the Under Secretary of Defense for Intelligence and Security, Counterintelligence, Law Enforcement, and Security (OUSD (I&S), (CLS), the program provides governance and advocacy for insider threat programs across the DoD Components and Services supporting nearly 15 million personnel.

The program is dedicated to the pursuit of advanced capabilities integrated within DoD security reform and vetting efforts, and to the development of a well-equipped, trained, and vigilant workforce to protect DoD resources, personnel, installations, and other equities from insider threats.

The DoD Insider Threat Program provides strategic oversight, issues policy and implementation guidance, and advocates for resources for the DoD Insider Threat community.

The office has played a critical role in advancing the mission through targeted investments in training and workforce professionalization and in advanced social and behavioral science research. The program also facilitates information sharing, collaboration, and continuous improvement of the insider threat discipline for stakeholders across the U.S. government and key partners in critical infrastructure.

For more information contact the OUSD(I&S) InT team's organizational box

osd.pentagon.ousd-intel-sec.mbx.dodcounterinsiderthreat@mail.mil

The U.S. Army Insider Threat Operations Hub is the operational element of the Counter-Insider Threat Program. It is designed to detect concerning behaviors from Army personnel and to deter, prevent, and mitigate threats to Army personnel, resources, and information.

The Hub utilizes Artificial Intelligence, Machine Learning, and other computer aided tools to identify behavioral patterns that may indicate an individual poses a risk to the Army.

Analysts compile information and consult with subject matter experts to assess risk and develop mitigation strategies.

The Hub further coordinates with "spoke" elements, including law enforcement, counter-intelligence, and security to ensure synchronized detection and response. We are proud to be the Army's first-line in detecting threats from within.

For questions or more information about the Hub, or to report concerning behavior, please contact:

usarmy.pentagon.hqda-dcs.mbx.g-34-int-hub-reports-cell@army.mil.

The MIROR JOURNAL
Managing Insider Risk and Organizational Resilience

The Managing Insider Risk and Organizational Resilience (MIROR) Journal

Produced and edited by the West Point Insider Threat Program
Published by West Point Press

FUNDING FOR THE MIROR JOURNAL

Provided by the Defense Counterintelligence and Security Agency, DCSA, and Undersecretary of Defense for Intelligence & Security, USD(I&S).

The West Point Press is the publishing arm of the US Military Academy, producing scholarly content for students, scholars, and leaders.

Our scholarly books, digital textbooks, journals, and other content reflect a commitment to the highest standards of scholarship.

WEST POINT PRESS

ABOUT

The Managing Insider Risk & Organizational Resilience (MIROR) Journal (Online ISSN 2832-5427 Print ISSN 2832-5419) is a scholarly Open Access journal published by the West Point Press, the publishing arm of the United States Military Academy, and produced by the Insider Threat Research Research Program at the Department of Mathematical Sciences at the United States Military Academy. The views expressed in the journal are those of the authors and not the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government. The mention of companies and/or products is for demonstrative purposes only and does not constitute an endorsement by the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government.

COPYRIGHT

OPEN ACCESS STATEMENT

Managing Insider Risk & Organizational Resilience (MIROR) Journal is an Open Access Journal which means that all content is freely available without charge to the user or his/her institution. Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the articles, or use them for any other lawful purpose, without asking prior permission from the publisher or the author. This is in accordance with the Budapest Open Access Initiative (BOAI) definition of open access.

The Managing Insider Risk & Organizational Resilience (MIROR) Journal does not charge authors for submission, processing, and publication.

REPOSITORY POLICY

Managing Insider Risk & Organizational Resilience (MIROR) Journal is an Open Access journal and supports the author's self-archiving their manuscripts/articles on their personal or institutional website, university, specialized repositories such as ArXiv.org, and research sharing websites such as ResearchGate. Authors are allowed to deposit their works after it has been published in the Managing Insider Risk & Organizational Resilience (MIROR) Journal, either online or in print, with no embargo. Authors can publish submitted, accepted, published manuscript/article, or publisher's PDFs.

ARCHIVING POLICY

Managing Insider Risk & Organizational Resilience (MIROR) Journal allows anyone to archive the content. The MIROR Journal will ensure long-term open access to the content by uploading the content to the Department of Defense digital repository DTIC (Defense Technical Information Center) DoDTechipedia public collections, Internet Archive (Archive.org), and deliver the printed journal to the Library of Congress.

The MIROR JOURNAL
Managing Insider Risk and Organizational Resilience
Volume 2 | Number 1 | Summer 2024

WELCOME

A SENIOR LEADER PERSPECTIVE

PROFESSIONAL COMMENTARY

The West Point Insider Threat research team at the 2024 Math Research Symposium (MaRS)

Front row: MAJ Carrie Donoho (Research Facilitation Lab); PhD, Cadets Sydney Watson and Kayla Teuscher; Dr. Pedro Wolf (RFL)
Second: LTC Russell Nelson, PhD; COL Joseph Lindquist, PhD; Cadets Joshua Blackmon, Samin Kim, Saleem Ali; Dr. Charles Hogue (Uniformed Services University for the Health Sciences)
Back: MAJ Hayden Deverill and LTC(ret) Jon Roginski, PhD

The MIROR JOURNAL
Managing Insider Risk and Organizational Resilience

Volume 2 | Number 1 | Summer 2024

ORIGINAL RESEARCH

LESSONS LEARNED AND CASE STUDIES

SUBMISSIONS AND CALL FOR PAPERS

WELCOME

Workforce Protection: The Next Generation of Insider Risk Programs

Stephanie L. Jaros
Applied Research Laboratory for Intelligence and Security (ARLIS)
at the University of Maryland

Jonathan W. Roginski
United States Military Academy at West Point

Since 2011, our community has successfully transformed Insider Threat Programs from reactive, often collateral duty assignments into a critical mission area focused on prevention, wellness, and collaboration. Along the way we have established a professionalization roadmap that includes a global certification and a graduate certificate, and we have educated our colleagues, supervisors, and agency leaders. Today, in 2024, insider risk professionals are members of a multi-disciplinary, global community committed to research-based policies, risk-based decisions, and ethical operational practices that fortify our organizations against current and emerging threats. In short, we protect our workforce.

Approximately 37 million Department of Defense personnel have worked between five and six billion hours since President Obama signed *EO 13587*.

> **Workforce Protection...accurately represents the work that we are doing...it summarizes our approach to risk management...**

Fortunately, during this same period, we experienced and recovered from only a small number of high-impact insider threat events. Rare events present several programmatic and measurement challenges, and so in recognition of this reality, Insider Threat Programs moved away from predictive threat models toward risk management practices, and several groups relaunched as Insider Risk Programs.

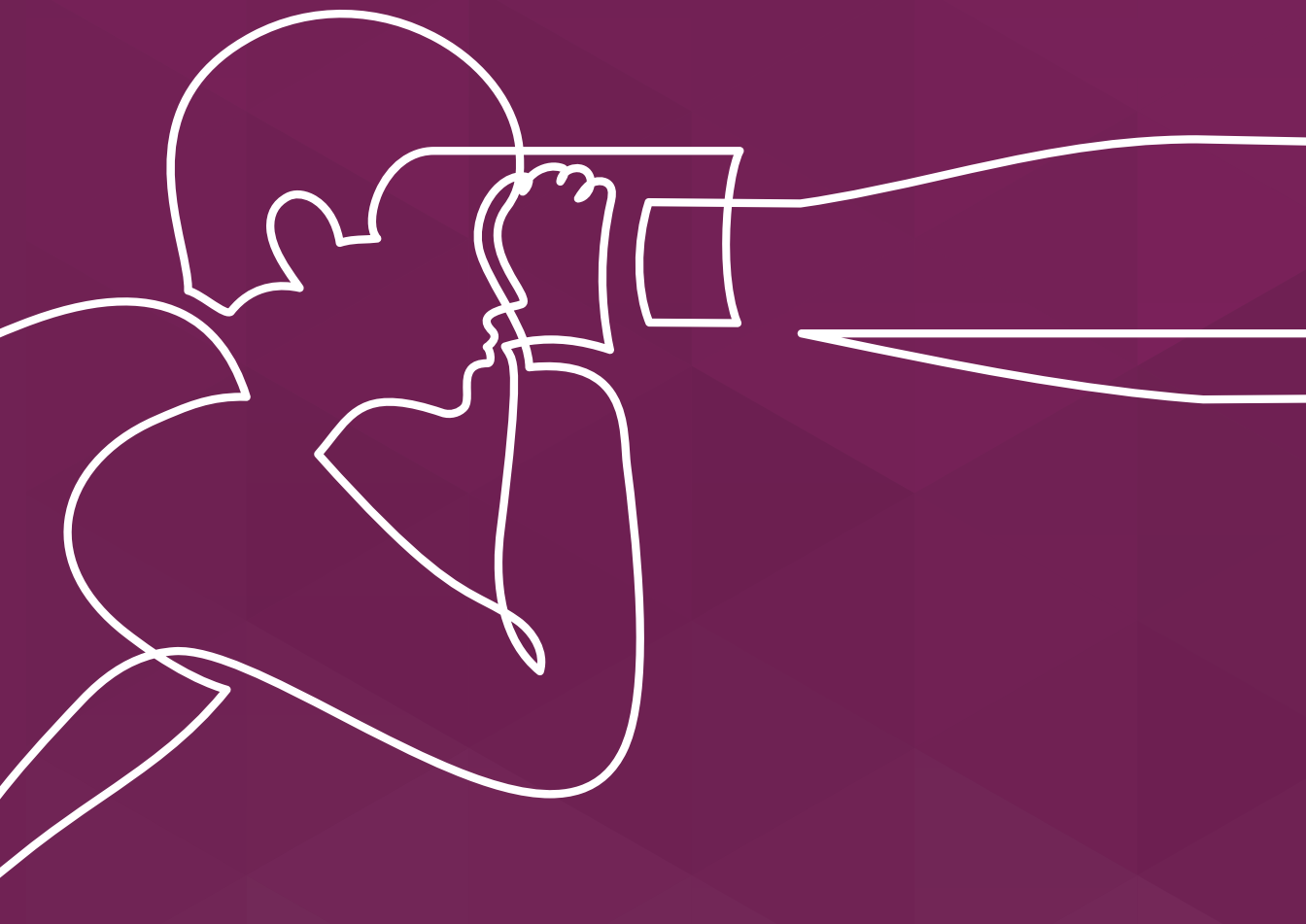
While this change marked a meaningful step, it is not enough. "Insider Risk" still implies that risk resides only within the individual and suggests that if we remove the person from our agency, we remove the risk. This is not how we measure success. "Insider Risk" ignores the organizational factors that we know contribute to concerning behaviors that persist even as employees come and go. Also, it continues to evoke thoughts of constant surveillance and confrontation. "Workforce Protection," in contrast, accurately represents the work that we are doing in our Hubs. It summarizes our approach to risk management, which includes our efforts to identify and mitigate both individual and organizational issues, and our attention to the full career life cycle. We believe this change once again will move our mission and our community forward because it captures our holistic approach and hopefully, inspires continued innovation.

Stephanie L. Jaros
Visiting Research Scientist & Insider Risk Consultant
sjaros@arlis.umd.edu
Follow me on LinkedIn

LTC (ret) Jonathan W. Roginski, Ph.D.
Program Manager, Insider Threat
jonathan.roginski@westpoint.edu
Follow me on LinkedIn

DISCLAIMER

The information and views expressed in this presentation are solely those of the author and do not represent opinions and policies of the Department of Defense, U.S. Government, U.S. Special Operations Command, the Joint Special Operations University, or the institutions with which the author is affiliated.



A SENIOR LEADER PERSPECTIVE

Diversity in Insider Threat Programs: Crucial to Mission Success

Henry Nelson

"Diversity is a mission imperative." That's what senior leaders across the Intelligence Community and Department of Defense have been saying for years, from Congressional hearings to workforce messages. Insider Threat Programs are part of dynamic and constantly evolving mission space that must change as rapidly as the threat landscape. So, how does diversity in those programs benefit that mission?

Threats are becoming increasingly sophisticated, requiring a diverse set of skills to proactively combat them effectively. By bringing together individuals with expertise in areas such as counterintelligence, human resources, cyber, law enforcement, security, threat assessment/threat management, and behavioral health, it heightens the opportunity for a holistic approach to insider threat detection and mitigation.

As insider threat tradecraft has evolved, the focus has been primarily on technological mitigations. We look for ways to speed up the evaluation process, to make informed decisions using corroborated and validated data, and to more thoroughly vet and resolve potential concerns. Many of these are reactive measures as we strive to keep pace in this 21st century threat environment. We have seen what happens when cleared individuals go out of their way to subvert our processes and security posture. It's our duty to stop them.

> **We know that diversity of thought and experience is a unique superpower when it comes to analysis – and the same is true for insider threat programs.**

HENRY NELSON

Henry Nelson serves as the Deputy Director, Enterprise Programs at the DoD Insider Threat Management and Analysis Center (DITMAC). In this capacity, he oversees and executes key offices, including the Assessment and Professionalization Office (APO), Unauthorized Disclosure Program Management Office (UD PMO), Mission Integration Office (MIO), and the Performance, Requirements, Information, Standards, and Metrics (PRISM) Office. Prior to his role at DITMAC, Mr. Nelson held the position of Chief, Counter Insider Threat Investigation Division at the National Geospatial Intelligence Agency (NGA). There, he successfully managed NGA's unauthorized disclosure program, leading a diverse team in two locations, and pioneered the integration of modernized investigative techniques, incorporating data science to detect, identify, and mitigate potential or actual threats to NGA personnel, resources, and information.

That is why diversity is so important in this field and why a multifaceted approach is necessary. Diversity goes beyond representation of different cultures and races; it also extends to a range of backgrounds, skill levels, technological aptitudes, educational levels, generational differences, and career disciplines. We know that diversity of thought and experience is a unique superpower when it comes to analysis – and the same is true for insider threat programs.

Diversity among insider threat programs gives us lots of advantages. First, it enables us to uncover vulnerabilities and threats that might not be readily apparent. These diverse perspectives enable a more nuanced and individualized approach to implementing mitigation strategies. For example, throughout the Defense Department, we have experts in Russian, Middle Eastern, and Asian affairs. Why do we have these experts? To comprehend the nuances of different cultures to facilitate the refinement of our tools, techniques, and procedures. Second, it allows us to explore a wider range of appropriate mitigation strategies and potential countermeasures, which gives us a more comprehensive understanding and assessment of risks.

This is especially important with a continuously evaluated, trusted workforce. People and culture change over time, so it's vital that we are able to discern and differentiate between life events that might be cause for concern or action versus those that are simply part of life. For example, integrating the expertise of a behavioral scientist or mental health professionals, can help insider threat programs better understand personality dynamics, social stressors, and the intersections of these on behavior – and that enables us to better assess and mitigate risk.

Beyond the practical advantages, fostering diversity within insider threat programs just makes sense. For insider threat programs to be effective in protecting our country, our people, and our resources, we must equip them with every possible advantage. We must fill them with creative, diverse people. We must give them the resources to integrate the latest technology. We must ensure they are prepared, at every moment, to adapt as threats emerge and to stay a step ahead of those who might harm our national security. Diversity – in all its forms – is a strategic and tactical advantage we cannot afford to overlook.

> **Diversity goes beyond representation of different cultures and races; it also extends to a range of backgrounds, skill levels, technological aptitudes, educational levels, generational differences, and career disciplines.**

PROFESSIONAL COMMENTARY

Mission First, People Always: Three Ways to Elevate Your Insider Threat Program Using Protective Intelligence

Ryan Matulka

Mission first, people always. This statement, often used in the military, encapsulates the tension between mission accomplishment and its potential human costs. Likewise, reducing insider risk and mitigating threats from organizational insiders can be a daunting task complicated by tradeoffs. Some organizations attempt and struggle to establish effective insider threat programs, challenged to not only obtain the buy-in of their people, but also to achieve a modicum of effectiveness.

There are common reasons these programs may fail to launch or under-deliver: misunderstanding, reactivity, and diffusion of effort. Threat and risk deterrence, detection, and mitigation programs are frequently perceived as adversarial in nature or overly invasive. "Big Brother" is watching me and wants to fire me. This is exacerbated by euphemistic program names which may seed cynicism and erode trust. Often sold as a "proactive" security, an audit of actual insider threat hub practices may reveal an exclusive focus on reactive incident response. We are categorizing what has already happened. When the specialized capabilities of the insider threat team are directed towards more common security matters lacking a clear insider nexus, it will likely reduce effectiveness in their primary domain. Organizations reduce bias in results, tunnel vision, and undesirable outcomes by effectively employing all assets in their intended manner.

> **"Prioritizing one group's interests or discounting another's too heavily is a blueprint for failure. Common ground between internal stakeholders can be achieved by tailoring the insider threat program activities to support the top priorities of the organization.**

RYAN MATULKA

Ryan Matulka is Senior Manager of Cyber Threat Intelligence and Insider Threat at Pacific Gas and Electric Company, one of the largest utility companies in the United States. There he built the company's first insider threat program from scratch. Previously, he served in the U.S. Army as a Special Forces Officer, Unconventional Warfare expert, and master planner responsible for advising and leading foreign and joint military forces. Ryan is a graduate of the United States Military Academy at West Point. He earned an MBA from the UCLA Anderson School of Management and a Graduate Certificate in Cybersecurity Incident Response from the SANS Technology Institute.

Given the human and operational resources at stake, leaders and employees are right to ask tough questions about their insider threat programs.

- **Whose interests does the program serve?** Does it serve investors, customers, employees, or a combination of all of them?
- **What is the goal of the program?** Is the desired outcome to find and mitigate threats, or to keep the company safe and secure? Does the first result in the second?
- **When do we intervene?** Should we intervene in a personal matter if the company has yet to be harmed? What is our duty to act if no policy has been violated yet but there is evidence of risk? Beyond our duty, do we have a responsibility to our people?
- **How do we balance protecting the company with protecting employees?** Is this a zero-sum game between the employer and its employees?
- **Do we trust employees?** Are employees the company's greatest asset or its greatest vulnerability? Or both?

The discussion around these questions is likely to reveal the internal tradeoffs between security, risk, and business objectives inherent to a complex organization. Prioritizing one group's interests or discounting another's too heavily is a blueprint for failure. Common ground between internal stakeholders can be achieved by tailoring the insider threat program activities to support the top priorities of the organization. As such, striking this balance between security and functional business perspectives is paramount for insider threat leadership.

> **Protective intelligence teams do not wait for precipitating events to act. Instead, they take the initiative to analyze past incidents, recognize emerging indicators, reduce vulnerabilities, and improve resilience.**

Despite the abundant programmatic hazards, there are clear models for success, such as a people-centric, protection mindset. According to the Cybersecurity and Infrastructure Security Agency (CISA), the core principles of successful insider threat mitigation programs are "***promoting a protective and supportive culture***," "***safeguarding organizational valuables***," and "***remaining adaptive***." These focal points in CISA's Insider Threat Mitigation Guide foster clear thinking about the most important feature of insider threat programs – the protection of people and organizational interests.

Safety and protection are foundational individual needs and are universally desirable. In the enterprise context, they are essential elements of responsible management. Stated as operating tenets of an insider threat program, these protective principles may be more likely to achieve buy-in than negatively-framed objectives such as "deter threats" or "detect malicious behaviors."

The protective intelligence discipline, like that practiced in the executive protection context, offers a transferrable and repeatable framework to achieve CISA's core principles for successful insider threat programs.

What is Protective Intelligence?

Security practitioners will not find a uniform definition of protective intelligence in professional bodies of knowledge. At a basic level, protective intelligence is simply an investigative and analytical method to proactively identify, assess, and manage threats. There are however several characteristics which set it apart from other security specializations.

The defining attribute of protective intelligence tradecraft is a continuous and ongoing effort to mitigate potential threats well before any adverse effects are realized. Protective intelligence teams do not wait for precipitating events to act. Instead, they take the initiative to analyze past incidents, recognize emerging indicators, reduce vulnerabilities, and improve resilience. Protective intelligence requires a different mindset than some other security disciplines.

Protective intelligence is most frequently applied to protecting high-profile individuals known as "principals," but it need not be limited to this. A compelling question for insider threat professionals is how to expand the beneficiaries from specific individuals to what CISA calls "organizational valuables" – i.e., groups of people, information, intangible assets, physical property, and by extension, the shared interests between groups of stakeholders.

Let's consider how to achieve a protective insider threat culture by examining three key ideas taken from protective intelligence and how they can be applied to insider threat mitigation.

Idea #1: Embrace the Intelligence Cycle

Advances in technology and the behavioral sciences have created a world where insider risk is reasonably foreseeable. Business and security technologies, with identity-based logging, monitoring, and auditing – standard in any modern enterprise – has enhanced the observability of behavioral indicators that would have been undetectable a few decades ago. Furthermore, researchers have developed and tested Structured Professional Judgment (SPJ) instruments which can improve the assessments of security practitioners when applied to individual cases. No one can forecast human behavior, but the use of comprehensive data and tested behavioral models raises the bar for what insider threat programs can achieve. With the substantial insights generated by the marriage of technology and expert human judgement, organizations have a duty of care to proactively manage insider risks.

Protective intelligence, guided by the intelligence cycle, is a way to carry out that duty of care. Intelligence methods are more suited to upfront, proactive work than the traditional "means, motive, and opportunity" investigative

approaches. Protective intelligence is not a substitute for investigations, rather they are complementary.

Protective intelligence starts with an intelligence requirement defined by a decision maker, whereas an investigation is predicated upon an allegation. Protective intelligence produces an assessment that may feed into the investigatory process. A completed investigation produces fact-based findings that can further inform intelligence requirements. Protective intelligence is future-oriented, whereas investigations focus on historical evidence. These subtle, but powerful distinctions put control back into the hands of protective intelligence specialists, allowing them to react less and protect more.

Figure 1. The Intelligence Process

Source: JP 2-0, Joint Intelligence

Idea #2: Elevate Analytical Thinking

The term "false positive," and other binary classifiers, have found their way into the insider threat lexicon, likely through the use of cybersecurity detection tools by insider threat teams. "False positive" means the misclassification of an object by a binary test with only two possible outcomes. Binary tests are appropriate for narrow applications with measurable and distinct criteria. Complex human behavior, on the other hand, should not be reduced to a binary test.

Using binary classifiers to describe human threats is an easy habit to form. Perhaps this is because binary tests can be automated or the terminology may imply precision and certainty. Caution is advised. If simple binary tests are normalized for insider threat practice, it may displace the laborious, but more relevant, expert assessments that require consideration of the totality of the facts. In its worst manifestation, binary thinking can overcome critical thinking. This may reinforce the natural tendency toward bias and cognitive shortcuts and become the acceptable path of least resistance. Lazy thinking is in direct opposition to CISA's first core principle, to build a protective culture. It can cause actual harm.

The management of cognitive bias is built into analytic tradecraft. Protective intelligence-based thinking strives to recognize and alleviate the errors that can creep into any analytical process. Protective intelligence analysts produce threat assessments based on the totality of the observable facts. When categorization of threats is required, it relies on scientifically-developed and tested SPJ instruments. These tools provide a defensible and repeatable way to make sense of large volumes of

evidence and case data. Cultivating a cross-functional team with diverse perspectives and recognizing the limits of one's professional experience and knowledge are two cognitive safeguards integral to Threat Assessment and Management, a key function of protective intelligence teams.

Protective intelligence requires its practitioners to acknowledge and describe uncertainties rather than simplify them through algorithmic and technological paradigms. Used appropriately, technology accelerates visibility and is a necessary part of any modern security posture. The most effective Insider threat leaders balance technological influences with both analytical and procedural approaches—and place human decision makers in the loop. The use of analytic confidence and estimative language to portray the natural ambiguity inherent in human behavior is more defensible than arbitrary and logical classifiers. Models and algorithms do not make decisions about people. People use the wisdom borne of experience and training to make decisions about people.

Idea #3: Reward Protective Outcomes

A protective intelligence approach to managing insider threat programs naturally facilitates a broader range of organizational responses to risk. In the protective intelligence model, success is defined as protecting the "principal" from harm, not

necessarily imposing consequences on a potential threat. Many insider threat hubs measure their success in terms of cases, investigations, and administrative actions. Discipline remains one of many tools available to management. However, if these are the only tools, there will be missed opportunities to create a positive organizational culture resultant from the most successful programs.

Building this flexibility can be accomplished by promoting the supportive side of threat assessment and management. This may include education, awareness, benefits, and services provided to subjects, victims, bystanders, and internal customers. Other noteworthy protective outcomes include remediation of vulnerabilities, creating awareness of threats, driving policy and procedural enhancements, and modifying behaviors through positive reinforcement.

Positive and negative incentives are not mutually exclusive. Both are useful risk mitigation tools and should be preserved as response options. But it is helpful to differentiate the influence of each through the framework of loss aversion. Discipline and adverse actions may be more likely to be perceived negatively by employees and by management. Even if a termination action is necessary and justifiable, should it be viewed as a "success?" It more likely to be viewed as a near-hit, a "cost," or a loss, depending on the circumstances and culture of the organization. On the other hand, outcomes where protecting people, data, and assets was the primary result, may be viewed as "wins" or as demonstration of return on investment (ROI), especially if the insider threat program is focused on the highest organizational priorities. Reframing the success criteria of insider threat programs may require effort to educate stakeholders, but the protective outcomes are more likely to catalyze human-centric stories which can better engage employees and the senior leaders alike.

"Reframing the success criteria of insider threat programs may require effort to educate stakeholders, but the protective outcomes are more likely to catalyze human-centric stories which can better engage employees and the senior leaders alike.

Lastly, thinking more broadly and inclusively about protection will help expand the mindset from threat to be more inclusive of risk. Consider a hypothetical situation where an employee is susceptible to coercion from adversarial foreign interests. The employee has not done anything wrong. There is no evidence of exploitation. They may not even be aware of their vulnerabilities. Security can highlight the potential bad outcomes, management can set expectations, and human resources can provide the necessary resources. This orchestration motivates a level of internal coordination that not likely to result from a narrower focus on malicious behaviors. The natural result of emphasizing protection will allow the company stakeholders to converge around their shared responsibility of protecting common interests.

Conclusion

These three ideas derived from the field of protective intelligence are useful for the insider threat discipline. They have practical and immediate benefits which may enhance performance and drive positive results. But also, they do more to contribute to a culture of support, trust, and safety than the necessary but grim work of finding and neutralizing threats. The modern organization and its insider threat program team have their work cut out for them. The mission is dynamic and complex. When they protect people first, everything else will fall into place.

Safeguarding "By, With, & Through" in Strategic Competition: A SOF CI Professional's Perspective

Michael W. Parrott

> Insider threats tear the fabric of trust built between partner forces.

Introduction

U.S. Special Operations Forces (SOF) across the globe often integrate into their operational environment by facilitating partner force engagements through a comprehensive approach that accomplishes the mission at hand. This "by, with, and through" concept is an essential part of America's diplomatic and military power projection. Nowhere is this more evident than in strategic competition, which requires leveraging relationships with allies and partners, to contend with challenges from other states and actors that include the People's Republic

MICHAEL W. PARROTT

Michael W. Parrott serves as the Special Operations Forces Counterintelligence (CI) Integration Course (SCIC) Director at the Joint Special Operations University (JSOU), MacDill Air Force Base, Florida. He is responsible for the development, execution, and instruction of joint force special operations curriculum. He served as a U.S. Army Counterintelligence Technician and Chemical, Biological, Radiological & Nuclear (CBRN) Defense professional prior to his retirement after 24 years of service to the nation. He is a former special operations intelligence management professional. His work has appeared in the Tip of the Spear magazine, the Simons Center's Interagency, and Military Intelligence Corps Association's Vanguard journals. Parrott holds a Master of Arts degree in Strategic Security Studies from the College of International Security Affairs at the National Defense University, a Bachelor of Arts in Homeland Security with a concentration in Terrorism Studies from the American Military University, and an Associate of Applied Science Degree in Intelligence Operations.

of China (PRC), Russia, Iran, and Violent Extremist Organizations (VEO). However, contemporary SOF partner engagements can trace their lineage back to the Office of Strategic Services (OSS) during World War II.[1] The OSS explored the use of partisan forces (like the French Underground, but also similar efforts in many other places) to disrupt, deny, and exploit the Axis Powers. In working with resistance forces, OSS officers quickly discovered the dangers of what is commonly referred to today as "insider threats."

Insider threats tear the fabric of trust built between partner forces. Trust is not just an essential element for all SOF engagements; it is both the metaphorical and literal lifeblood for these partnerships as U.S. and Coalition forces learned in Afghanistan. In 2012, insider or "green-on-blue" attacks accounted for 15% of coalition force deaths.[2] Again, in 2019, green-on-blue attacks resulted in 172 killed and 85 wounded in 82 separate incidents perpetrated by Afghan soldiers and Taliban infiltrators.[3] In addition to lessons learned by the OSS, today's SOF must not abandon lessons learned from the past 20 years of counterterrorism. Instead, SOF must preserve these lessons and innovate new approaches to confront a more sophisticated insider threat challenge posed by strategic competitors.

The contemporary insider threat challenges SOF are faced with in partnering environments are not unique to special operations; insider threats discussed here can affect businesses, commercial entities, academia, and government institutions. However, the lessons to be learned from historical retrospection and ways to prepare and protect SOF members and their families now and in the future can also help leaders and security professionals in other industries. Many of

the lessons and recommendations outlined below can be applied more broadly by insider threat professionals in various sectors; the concepts apply to all organizations…government or civilian. Nevertheless, this article will focus predominately on the SOF nexus, while yielding helpful options for dealing with insider threat dilemmas outside the enterprise.

Contemporary Insider Threat Challenges

As USSOF prepares to train Mexican SOF members in 2024, the threat of attacks by cartel infiltrators or assets within the partner force continues to pose a similar threat to insider attacks in Afghanistan by co-opted Afghan security forces and partner force members. The costs can be very high, as demonstrated by a 2019 insider attack in which "a Taliban infiltrator killed 23 Afghan National Army soldiers in their sleep."[4] SOF were not immune to such attacks. In early 2020, members of 7th Special Forces Group (7th SFG) and allied Afghan Special Operations Forces were conducting a key leader engagement with influential figures in the Sherzad district of Nangahar province. The post incident report indicated the insider attack occurred when, "an individual in an Afghan uniform opened fire on the combined U.S. and Afghan force with a machine gun," resulting in multiple U.S. and Afghan casualties.[5]

Ruthless Mexican cartels – threatened by government security forces and now USSOF trainers (from 7th SFG) – could employ similar tactics.[6] In the late 1990s, the Gulf Cartel convinced over 30 Mexican military members to form a group commonly referred to as Los Zetas.[7] Again, in 2023, Mexican military officials were thrust into the media spotlight as millions of SEDNA (Mexico's Defense Department) documents that contained evidence of collusion between high level military officials within the department and drug cartels were leaked by trusted insiders.[8] In parallel, cartels have also retaliated against host nation security and police officers. In December 2023, cartels killed Mexican police officers believed to have stolen cartel drug shipments.[9] Cartel infiltration, coercion, and brutal tactics paint a grim operating environment, analogous to Afghanistan between 2010 and 2019.

> "As tensions rise, insider risk heightens and the potential for insider attacks grows

To confront these challenges, an examination of insider incidents and lessons from Afghanistan can help mitigate risks associated to comparable threats today. Continuous vetting, counterintelligence integration, guardian angels, and various assessments helped fetter out insurgent infiltrators in Afghanistan and Iraq. On July 7, 2018, U.S. Security Force Assistance Brigade members succumbed to an insider attack near Tarin Kowt Airfield, Afghanistan. The investigation revealed the quick actions of U.S. soldiers, referred to as Guardian Angels, "played an invaluable role in minimizing the number of casualties," according to the investigating officer's report.[10] The attacker, an Afghan National Army soldier, had no clear motive, which highlighted flaws in the Afghan military's vetting process. Post-attack interviews uncovered that the number of individuals to be vetted overwhelmed the system; many made it through the initial screening process without undergoing the necessary scrutiny or vetting required.[11] All the more reason Coalition Forces employed a continuous vetting process for partner forces and locally-employed persons. A process that enabled security forces to discover connections between trusted insiders and nefarious actors that may have been missed during initial screening interviews or later after an insider was coerced, intimidated, or manipulated by Taliban or insurgents to switch sides. Another technique that proved fruitful was the use of biometrics devices.

Biometric enrollment and screenings of Afghan National Security Force personnel were part of the vetting and recruitment process for all members of the Afghan National Defense & Security Forces.[12] These devices denied anonymity to would-be infiltrators while counterintelligence interviews helped U.S. and coalition forces identify aspiring attackers and adversarial collectors. An assessment by the Special Inspector General for Afghanistan Reconstruction reported no insider attacks nor casualties occurred among U.S. and Coalition forces during the last few months of 2020, which reinforces the additional protective measures instituted helped deter or dissuade insider attacks.[13] However, a key difference between Afghanistan and Mexico is proximity to the U.S. homeland.

The proximity and reach cartels exhibit not only endangers USSOF members in Mexico, but also their families in the U.S.[14] This additional dynamic exacerbates an already complex threat environment for USSOF. USSOF employs counterintelligence professionals to protect, exploit, and neutralize foreign intelligence entity threats at home and abroad. They should undoubtedly play an important role when USSOF elements deploy to Mexico next year. Through effective CI integration and partnerships with U.S. federal, state, and local law enforcement agencies, the threat of cartel retaliation and/or reprisals against USSOF members and families can be identified and neutralized. Border Enforcement Security Task Force (BEST) teams, led by U.S. Immigration and Customs Enforcement (ICE), employed along the southern border have proven to be a useful capability in response to cartel violence and activities

affecting both Mexico and the U.S.[15] The BEST teams have successfully partnered with Mexican law enforcement to interdict and apprehend hundreds of criminals and their illicit cargo. Similarly, the U.S. Drug Enforcement Administration (DEA) uses vetted units. These Sensitive Investigative Units (SIU) leverage trained and vetted foreign police officers to cooperatively investigate specific cases within the host nation that have a U.S. nexus.[16] Therefore, it is incumbent on USSOF leaders to incorporate proven lessons from Afghanistan and throughout history to mitigate insider threats in partnering environments, especially as they prepare to work in Mexico and other high-threat countries.

Strategic Competition and the Insider Threat in Taiwan

Although the U.S. should not abandon lessons already learned, it must anticipate and innovate to address insider threats in a new strategic environment. Nowhere is this challenge more apparent than in USSOF-partner engagement in Taiwan. USSOF continue preparation and training initiatives with Taiwanese counterparts as PRC hostilities mount.[17] Partnerships like these make it increasingly difficult for the PRC to subvert the Taiwanese government or its people; however, they also present opportunities for exploitation, infiltration, co-option, or worse by PRC intelligence and security services.[18] USSOF must adapt to a CI environment more familiar to their predecessors' experiences during the Cold War than the more recent Global War on Terror.

PRC espionage activities in Taiwan are formidable. Peter Mattis and Matthew Brazil have examined decades of spying by Taiwanese individuals and groups on behalf of the PRC and espionage plots involving Taiwanese military members from all echelons up to the three-star level.[19] In 2017, Taiwanese national security officials estimated approximately 5,000 individuals were spying for the PRC in Taiwan.[20] This number continues to grow. From 2002 to 2020, Taiwanese authorities uncovered 60 espionage plots that could be just the tip of the iceberg—and affect those at the tip of the spear.[21] For instance, in August 2023, a Taiwanese pilot was arrested and charged with spying for China, after attempting to steal and defect with a U.S.-made CH-47 helicopter, a workhorse for USSOF, in exchange for $15 million dollars.[22] The arrests of both the pilot and a retired Taiwanese military officer occurred because of a tip-off. A tip, most likely, resulting from Taiwan's aggressive counter-espionage campaign focused on education, awareness, and reporting.[23] Had the PRC acquired the airframe, the People's Liberation Army (PLA) would undoubtedly have reverse-engineered it to fill a gap within the army's current fleet.

Trust is critical to effective partnerships. USSOF members must build trust and relationships with Taiwanese counterparts despite the heightened risk of operating in a critical insider threat environment. The dilemma of how much to reveal versus conceal in working with partner forces place SOF personnel in a precarious position. USSOF currently face the challenge of PRC espionage by proxy through partner engagements. The Global Taiwan Institute asserts that "Taipei has no way–short of accepting unification–to stop Beijing's human and technical intelligence operations."[24] PRC intelligence services target and exploit current and former Taiwanese military and government officials. They have also started using university students to spy within the island nation. The addition of academics and students resembles efforts by the PRC to recruit students studying in the United States, via the Thousand Talents Program, to spy on China's behalf.[25] A practice that is proving fruitful and difficult to detect, exploit, or neutralize. European nations, like Germany, are even sounding the alarm on the unprecedented influx of Chinese students, an "Army of spies".[26] Additionally, in November 2023, 10 active-duty and retired military personnel were indicted by Taiwan on suspicion of spying for China.[27] Currently, insider threat trends within Taiwan focus on political influence, subverting the will to fight, and technology exploitation on behalf of the PRC. A concern for the U.S. defense industry and a wake-up call for USSOF leaders; a clear threat to SOF's competitive advantage.

As tensions rise, insider risk heightens and the potential for insider attacks grows. In the event of hostilities between the PRC and Taiwanese and/or U.S. forces, the PRC could leverage networks of insiders to sabotage or attack Taiwanese defense and resistance structures and organizations. To confront the operating environment's challenges, USSOF can and should remain vigilant and resilient to the effects and

impacts insider threats may have on operations, personnel, and partners while limiting the damage that counter-insider threat and counterintelligence efforts can inflict on trust, the *sine qua non* of effective USSOF partnerships.

Mitigating Insider Threats in Partnering Environments

Studying the trends experienced in Afghanistan and during the Cold War can provide USSOF and other government, commercial, and private sectors with valuable insights to help confront insider threats in partnering environments. In Afghanistan, U.S. military leaders sought solutions to green-on-blue attacks. They turned to the U.S. Army's Asymmetric Warfare Group (AWG) for help. The group provided recommendations and useful tools for leaders to use to mitigate the risks associated with partnering with foreign forces. These same tenets and elements can be used to guide intra-organizational insider threat programs as effectively as between organizations. Often, different "branches" of organizations--especially large organizations--have different perspectives, missions, needs, and priorities. The branches must "partner" for an effective insider threat program within the enterprise. This is something we can build upon to connect DoD and non-DoD perspectives.

In June 2011, the AWG created a useful infographic titled, "Insider Threats in Partnering Environments: A Guide for Military Leaders." AWG's guide assists in three areas: awareness, information, and dialogue between US and partner force elements.[28] The guide states that partnering "in itself is a sensitive mission and only by creating trust and having an open dialogue with all forces will the mission be accomplished."[29] To overcome the insider threat the guide provides leaders with observable indicators and decision matrices to assist leaders and staffs with determining acceptable risk categories and mitigation procedures. While there is little to no definitive proof this guide contributed to reduction in the number of insider attacks in Afghanistan two years after it was implemented or if some other factor(s) were to blame. The guide still provides helpful recommendations USSOF leaders should review, and institute as they prepare for partner force engagements in 2024 and beyond.

A retrospective examination of World War II and Cold War era archives provides a treasure trove of useful examples of compromised networks and insider threats applicable to today's strategic competition and partnering environments. In 1942, the United Kingdom's Special Operations Executive (SOE), the British counterpart to America's OSS, experienced one of its most significant compromises of WWII.[30] German security and Nazis captured over 50 clandestine SOE agents in Holland and compromised the entire operation by penetrating the newly formed Dutch resistance forces.[31] In France, over 80 separate resistance groups were established by British Intelligence's special division, commonly referred to as F-Section.[32] The SOE's Prosper Mission, which F-Section played a critical role in, employed Henri Dericourt, a French military officer to secretly control air traffic into the Paris area of operations for the network of spies, saboteurs, and operatives.[33] Unbeknownst to SOE and British intelligence was Dericourt's concealed connection to Hans Boemlburg, the chief of German counterespionage, which resulted in 14 clandestine airfield locations compromised and a number of agents captured, tortured, or killed.[34]

In contrast, Military Assistance Command Vietnam, Studies, and Observation Group (MACVSOG) missions in Vietnam resulted in a mix of success and failure. OP35, MACVSOG cross border operations in Laos and Cambodia, were highly effective "for a myriad of reasons including highly trained and motivated personnel, a depth of experienced in the exact missions they were going to conduct, exemplary leadership at multiple levels and immeasurable amounts of trust amongst those involved."[35] However, OP34s agent operations proved to be disastrous, "costing high attrition amongst the trained Vietnamese agents."[36] Mass training of potential agents and centralized housing of all recruited agents with trainees resulted in operational security degradation and compromise by those without the necessary need-to-know. Due to this mass training, MACVSOG had no way to determine or account for what information was divulged to the enemy by compromised partner

force members. A method that reemerged during the Operation Enduring Freedom-Afghanistan, when U.S. and coalition forces trained Afghan security forces en masse, a technique that should not be repeated in the current strategic competition environment within the INDOPACIFIC region.

Similarly, examination of the insider threats in Taiwan today presents distinct challenges and concerns. The language barrier forces USSOF personnel to adapt and develop organic language capacity or rely on contracted linguistic support; a problem shared by the commercial and private sectors. The latter poses an opportunity for PRC penetration, co-option, or coercion for Mandarin Chinese and Taiwanese speakers with families in mainland China. A review of motivations for espionage committed by PRC operatives proves that many reside within the private sector.[37] This creates opportunities to infiltrate and influence the human domain where USSOF are often interfacing and interacting within partnering environments at the spear tip. Like SOF operators – corporate executives and entrepreneurs – face comparable challenges when interacting with foreign business owners or operating in foreign markets.

Counterintelligence professionals within SOF formations or supporting elements can help detect, identify, exploit, and neutralize the threat actors and/or their activities. Additionally, counterintelligence personnel (in any organization) could liaise with host nation security and intelligence forces and resident U.S. interagency personnel to help deny anonymity and operating space to PRC intelligence and security forces seeking to exploit gaps caused by language, culture, or other means. In a recent 2023, *Tip of the Spear* magazine article, I emphasize that more effective counterintelligence integration within SOF is needed, a practice that is vital to countering foreign intelligence threats to USSOF in partnering environments.[38]

Conclusion – A CI Professional's Perspective

Over the course of my 24-year U.S. Army career it became clear that engagements with foreign partners proved to be built on trust, mutual respect, and a fellowship of comrades-in-arms. As a counterintelligence professional, it was necessary to protect the force while ensuring the mission's success without compromising the trust built between USSOF partners and their counterparts. This was often difficult, yet attainable. Many of the approaches and methods used to vet partners, while unorthodox, proved valuable years, even decades later. The implementation of Guardian Angels and counterintelligence interviews of questionable or suspected individuals proved positive and saved lives. Then and now, the adoption of new technological advancements in data management, biometrics devices, and analysis are speeding up the process. By simply gathering biometrics and pertinent assessment information early, it enables partners to be vetted faster. However, the human

factor is still must be considered. To build trust amongst partner forces it takes time and focus. Stephen Covey's book *The Speed of Trust* articulates why character and competence – two traits examined during SOF assessments and selection processes – are vital to building lasting partnerships (relationships).[39] The same can be said about corporate employee interviewing and screening practices. While the speed with which partners can be expedited through the verification process improves the overall amount of time spent training with USSOF members on mission-enhancing skills like shooting, rappelling, patrolling, etc. it is critical that trust is built and maintained throughout the partnership. Most mitigation measures can be implemented with very little effort or impact to the partnering mission. It is incumbent on leaders within USSOF to help educate their members on the need for counterintelligence integration into future events to ensure USSOF members, operations, activities, and investments are protected from foreign intelligence and insider threats in partnering environments. The same, can be said for corporate America that face insider threats from within and on the periphery in business ventures, similar to what SOF faces in partnering environments.

DISCLAIMER

The information and views expressed in this presentation are solely those of the author and do not represent opinions and policies of the Department of Defense, U.S. Government, U.S. Special Operations Command, the Joint Special Operations University, or the institutions with which the author is affiliated.

> it [is] necessary to protect the force while ensuring the mission's success without compromising the trust built between ... partners. This [is] often difficult, yet attainable.

REFERENCES

1. Diana I. Dalphonse, Chris Townsend, and Matthew W. Weaver Shifting Landscape: The Evolution of By, With, and Through. *The Strategy Bridge*. August 1, 2018. https://thestrategybridge.org/the-bridge/2018/8/1/shifting-landscape-the-evolution-of-by-with-and-through.
2. Bill Roggio & Lisa Lundquist. Green-on-Blue Attacks in Afghanistan: The Data. Real Clear Defense. March 21, 2017. https://www.realcleardefense.com/articles/2017/03/21/green-on-blue_attacks_in_afghanistan_the_data_111015.html.
3. Jared Keller. Insider attacks against US troops in Afghanistan have dropped too a historic low. Here's why. *Task and Purpose*. February 2, 2021. https://taskandpurpose.com/news/insider-attacks-afghanistan-2020/.
4. Jared Keller, 2 Feb 2021, https://taskandpurpose.com/news/insider-attacks-afghanistan-2020/.
5. James Laporta and Tom O'Connor. U.S. and Afghan Special Operations Forces Killed in Deadly Ambush. 8 Feb 2020. https://www.newsweek.com/us-afghan-special-operations-forces-killed-deadly-ambush-1486400.
6. Karol Suarez, The power of blood: Why Mexican drug cartels make such a show of their brutality. USA Today. 18 DEC 2023. https://www.usatoday.com/story/news/nation/2023/12/18/mexican-drug-cartels-brutality-power/71932898007/.
7. Samuel Logan. A profile of Los Zetas: Mexico's second most powerful drug cartel. Feb 2012, Vol 5, Issue 2. CTC Sentinel. https://ctc.westpoint.edu/a-profile-of-los-zetas-mexicos-second-most-powerful-drug-cartel/.
8. Armando Velasco. Mexico military hack shows revelations of cartel involvement with some defense officials. 18 OCT 2022. Fox News. https://www.foxnews.com/world/mexico-military-hack-shows-revelations-cartel-involvement-with-some-defense-officials.
9. CBS News. Cartel leaders go on killing rampage to hunt down corrupt officers who stole drug shipment in Tijuana. Insider attacks against US troops in Afghanistan have dropped to a historic low. Here's why. 12 DEC 2023. https://www.cbsnews.com/news/cartel-leaders-kill-corrupt-officers-who-stole-drug-shipment-tijuana-mexico/.
10. Kyle Rempfer. Investigation of 2018 green-on-blue attack criticizes vetting of Afghan forces, praises actions of US riflemen. *Army Times* magazine. 26 Jun 2020. https://www.armytimes.com/news/your-army/2020/06/26/investigation-of-2018-green-on-blue-attack-criticizes-vetting-of-afghan-forces-praises-actions-of-us-riflemen/.
11. Ibid.
12. Krystian Fracik. Insider attacks as one of the main threats to Resolute Support personnel in Afghanistan. *Security & Defence Quarterly* Vol 12, March 2016. https://securityanddefence.pl/Insider-attacks-as-one-of-the-main-threats-to-resolute-support-personnel-in-Afghanistan,103234,0,2.html.
13. Jared Keller. Insider Attacks in Afghanistan 2020. 2 FEB 2021. *Task & Purpose.* https://taskandpurpose.com/news/insider-attacks-afghanistan-2020/.
14. DEA. United States: Areas of Influence of Major Mexican Transnational Criminal Organizations. DEA-DCT-DIR-065-15. July 2015. https://www.dea.gov/sites/default/files/2018-07/dir06515.pdf.
15. Sigrid Arzt. U.S.-Mexico Security Collaboration. The Wilson Center March 31, 2023. https://www.wilsoncenter.org/sites/default/files/media/documents/publication/Chapter%2012-%20U.S.-Mexico%20Security%20Collaboration%2C%20Intelligence%20Sharing%20and%20Law%20Enforcement%20Cooperation.pdf .
16. Ibid.
17. A.B. Abrams. Building a U.S. Special Forces 'Stealth Network' on Taiwan. *The Diplomat*. 3 May 2023. https://thediplomat.com/2023/05/building-a-us-special-forces-stealth-network-on-taiwan/.
18. Stavros Atlamazoglou. US Green Berets who've trained Taiwanese troops explained how they could fight China and why the US keeps their mission secret. *Business Insider.* 24 OCT 2021. https://www.businessinsider.com/us-green-berets-explain-how-they-train-taiwan-troops-2021-10.
19. Peter Mattis and Matthew Brazil. *Chinese Communist Espionage: An Intelligence Primer*. 2019. Naval Institute Press, Annapolis, Maryland.
20. Chung Li-hua and Jonathan Chin. 5,000 Chinese Spies in Taiwan: Source. *Taipei Times.* 13 March 2017. https://www.taipeitimes.com/News/front/archives/2017/03/13/2003666661.
21. Ibid.
22. Peter Suciu. China Offered Taiwanese Pilot $15 Million to Steal U.S.-Made CH-47 Helicopter. 13 December 2023. https://nationalinterest.org/blog/buzz/china-offered-taiwanese-pilot-15-million-steal-us-made-ch-47-helicopter-207917.
23. Reuters. Taiwan boosts counter-espionage effort after suspected China infiltration. 2 Aug 2023. https://www.reuters.com/world/asia-pacific/taiwan-boosts-counter-espionage-effort-after-suspected-china-infiltration-2023-08-02/.
24. Peter Mattis. 28 September 2016. Spy Games in Taiwan Strait: Taipei's Unenviable Espionage Problem. Global Taiwan Institute. https://globaltaiwan.org/2016/09/spy-games-in-taiwan-strait-taipeis-uneviable-espionage-problem/.
25. Aaron Jensen. China Expands its Spying Against Taiwan. The Diplomat. 21 March 2017. https://thediplomat.com/2017/03/china-expands-its-spying-against-taiwan/.
26. Ritu Sharma. China's 'Army of Spies' Horrifies Germany; Report Cautions Against Massive Influx of Chinese Students. 3 January 2024. https://www.eurasiantimes.com/china-cranking-up-espionage-activities-in-germany/amp/.
27. Cindy Wang. November 23, 2023. Taiwan Indicted Military Person Suspected of Spying for China. https://www.bloomberg.com/news/articles/2023-11-28/taiwan-indicted-military-personnel-suspected-of-spying-for-china.
28. U.S. Army Asymmetric Warfare Group (June 2011) *Insider Threats in Partnering Environments: A Guide for Military Leaders*.

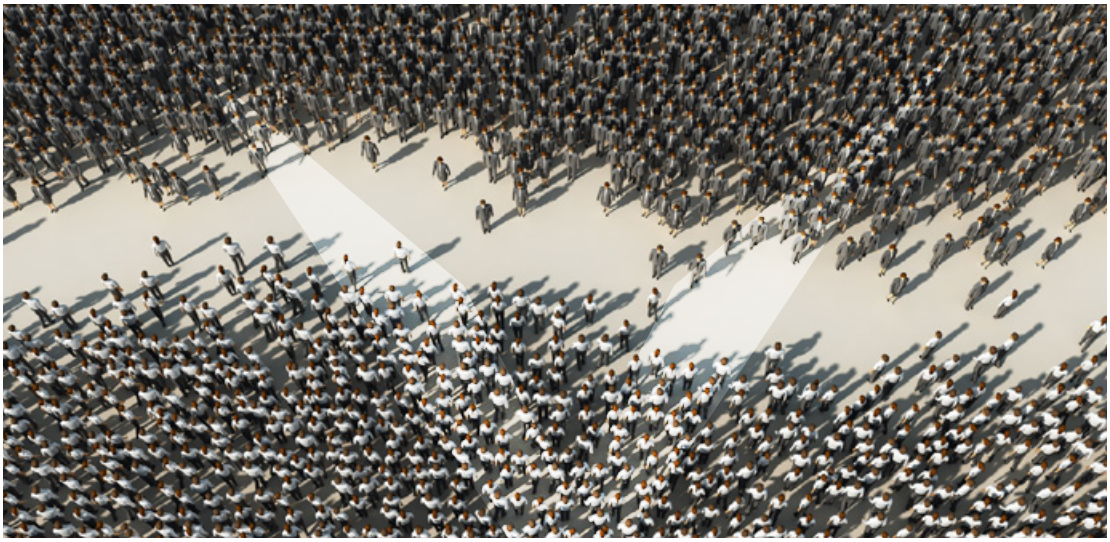
REFERENCES

29. Ibid.
30. Robert Hutton. Was this the UK's Worst Spy Failure of World War II? 13 May 2022. History Net. https://www.historynet.com/was-this-the-uks-worst-spy-failure-of-world-war-ii/.
31. Paul Lashmar & Chris Staerck. Spy fiasco cost Britain 50 agents. 21 September 1998. *Independent.* https://www.independent.co.uk/news/spy-fiasco-cost-britain-50-agents-1199631.html.
32. Peter Kross. The British Prosper Spy Network: Destroyed to Protect D-Day? September 2007. Warfare History Network. https://warfarehistorynetwork.com/article/the-british-prosper-spy-network-destroyed-to-protect-d-day/.
33. Ibid.
34. Ibid.
35. Daniel J. Staheli. Analysis of Military Assistance Command Vietnam, Studies and Observation Group (MACVSOG) Against the Special Operations Forces Truths. AY 2019-20. https://apps.dtic.mil/sti/trecms/pdf/AD1177859.pdf.
36. Ibid.
37. Nicholas Eftimiades, *China's Espionage Recruitment Motivations: Getting Rid of the MICE* European Intelligence Academy Research Paper Series #5 December 2023. https://www.rieas.gr/images/editorial/EIAPaper5.pdf.
38. Michael W. Parrott, *Foreign Intelligence Threats to SOF – Why Counterintelligence Integration is Vital.* October 2023. Tip of the Spear Magazine. https://www.dvidshub.net/publication/issues/68487.
39. Stephen Covey. *The Speed of Trust.* Pg 30. Free Press. Feb 2008.

Countering Insider Threat in a Fractious Society – a View from Australia

Timothy V. Slattery

Insider threat is an ancient phenomenon. People who betray the trust of those around them have always existed as thieves, embezzlers, spies, saboteurs: the disgruntled. Also ancient is peoples' tendency to live and work in groups, evolving to operate as an ordered community – as a society. Within society, insider threat is written into Western cultural artefacts (for example, Judas' betrayal of Jesus) and is recorded across the canon of Western history. Insider threat is endemic to the human condition.[1]



Editor's note

The MIROR journal and its staff are staunch believers in personal dignity and the essential equality of people at the human level, regardless of any demographic affiliation. This article is written from a Western, Judeo-Christian perspective. The content does not denote nor connote the superiority of any set of values over another. It is the author's honest viewpoint, perspective and commentary offered here as a safe space for discussion and honest discourse that moves our community together toward a safer, more tolerant existence.

TIMOTHY V. SLATTERY

Tim Slattery served in Australia's army, intelligence and national security community for 37 years. Tim has operational and policy experience across defence, intelligence, law enforcement and protective security domains, including with Five Eyes partners. Tim retired from Australian federal government service in 2019, joining the consulting community in 2020 with focus on insider threat and broader personnel security issues across government, critical infrastructure and private sector clients. Tim co-founded of Pentagram Advisory Pty Ltd in 2024 to better focus his efforts to promote understanding and mitigation of insider threat.

Whilst the phenomenon is ancient, contemporary insider threat in Western societies is arguably more virulent and more consequential than ever before. Why? The flattening of societies resulting from omniscient technology correlates with a decay in the influence of traditional societal pillars in unifying the populace. The pillars of Western (European) society are generally taken to be: the *Judeo-Christian tradition, democracy* stemming from ancient Athens (5th century BC) linked to the Enlightenment (17th and 18th centuries), and *rationality* stemming from the time of Aristotle (4th century BC) and linked to the Renaissance (15th and 16th centuries) and Reformation (16th century) which enabled science. Decay, in this situation means a reduction in the potency of entrenched guiding principles for Western societies to influence (and unify) the populace. This reality, coupled with historically rapid and transformative technological advances, has promoted social fracture and large-scale 'othering'.[2] Societies are decreasingly coherent and hence less likely to offer people common purpose.

This reduction in coherence—or unity—contributes to fracture within our society and provides the space for insider threats to take root, to propagate, to succeed, and cause catastrophic damage.

> *Leaders and managers must proactively counter contemporary insider threat to secure the asset or capability for which they are responsible. Leaders are charged with this duty in the face of a workforce drawn from a fractious society which encourages focus on self rather than the goals of the enterprise, to the detriment of society.*

Historical Context

Recent times have represented a set of historically unparallelled changes in society, occurring at an ever-increasing pace driven by technology. Stimulated by the Cold War, the United States' military-industrial complex continued a peacetime version of the societal mobilisation ignited in World War II. The United Kingdom underwent a scaled-down version of the US military-industrial complex. The U.S. yoked the needs of national security to the national economy serving its society, for example civil nuclear electricity production coupled to nuclear-powered and nuclear-armed submarines. The collaboration between government, business, science and society shaped by war delivered victory, the engine for ongoing security and significant benefits for society. Australia has maintained little such military-industrial capacity.

Also, in the wake of World War II, societies became less conservative, less constrained by norms that existed in the first part of the 20th century (there were glimpses of this in the 1920s post World War I). Growing post-war economies promoted consumerism, public health and expanded programmes of secondary and tertiary education which, by the 1960s, stimulated popular interrogation of societal pillars by people in Western democracies including Australia, the U.S. and the UK. *Post-modernism* developed in the 1960s amongst the humanities departments of Western academe and evolved to be a movement questioning the 'traditional': Christianity, ideologies such as Marxism, social class, science, and the pillars of post-Enlightenment Western democracy.[3]

Challenges to 20th century's societal pillars have left them weakened, and even replaced in some cases. Long-held viewpoints of the efficacy of democratic government, probity of Christian faiths and institutions, the honesty of banks and big business, the credibility of leadership hold less sway over members of society. Popular disquiet over the costs and morality attributed to national security has led many to find government to be questionable and untrustworthy.

Pillar beliefs that once made society strong became discredited. Innovative capitalism gave way to the 'greed is good' 1980s, a phrase attributed to the U.S. stock trader Ivan Boesky who was jailed in the 1980s for insider trading, with the phrase also recited by the character Gordon Gekko in Oliver Stone's 1987 film Wall Street,

> **Contemporary insider threat in Western societies is arguably more virulent and more consequential than ever before.**

emphasised materialism and the centrality of the individual, and when coupled with the social and economic globalisation of the 1990s ultimately eroded many people's trust in those pillars. Western blue-collar jobs were offshored and with them national security-relevant capabilities (military, industrial, scientific, information technology) were diminished as the end-of-the-Cold-War 'peace dividend' was harvested.

With the dust still settling from the fall of the Berlin Wall in 1989, the introduction of public internet in 1993 democratised access to information which, when coupled to the advances in consumer electronics (for example, 21 iterations of Apple iPhones 2007-2023), became a seminal historical conjunction enabling and empowering the individual over the state as never before in human history. This unbridled information access enabled individuals to contend with and potentially overcome the nation state and its societal institutions. Financial shocks in the 2000s and the recent COVID pandemic further untethered Western societies from established pillars because people could now, by virtue of powerful technology including home computing, entertainment and personal portable electronic devices, modify elements of their reality by 'on-demand' consumption of news, entertainment and information aligned to their desires and curated beliefs. Empowering research through quick access to vast troves of information nesting on the internet became available to all. Individuals have access in their hand to capabilities, such as overhead imagery and geolocation, that were the exclusive purview of select nation states a few decades before. Over the last 60 years people became tooled, and predisposed, to be activistic in their personal and work lives – almost untethered from the established pillars of society on which their forebears had relied – with consequences for their political, social, criminal, and tribal activities.

> *Leaders and managers need to understand recent history (many in their workforce won't) – the 'how we arrived at the current situation' – to provide context for the decisions they need to make today about the secure operation of their enterprise. To identify risk stemming from insider threat the enterprises' unique operating environment—including historical context—must be appreciated.*[4]

Changes in Society

The powerful changes in society, coupled with the explosion of technology-fueled rapid and chaotic change in Western societies, spawned an ever-dividing (increasingly fractious) society: a form of social meiosis based on differences. A lexicon has evolved to encompass a range of social inequalities and identity politics. Such terms became shorthand social descriptors generally relating to racial or social injustice,

in time evolving to diffuse political movements whose adherents embrace and identify with as strongly as a religiously devout person might have embraced their faith during the Western Protestant Reformation of the 1500s. Such terms merged with Postmodernism to derive the term *Social Justice scholarship*[5] which is a feature of Western democratic societies today, especially prevalent in universities.

In recent years, researchers and authors have explored the foundations and evolution of the features and consequences of personal beliefs that align generally to critical race theory, post-colonialism, social justice and identity. Two such books, *The Madness of Crowds: Gender, Race and Identity* by Douglas Murray (2019) and T*he Coddling of the American Mind* by Greg Lukianoff and Jonathan Haidt (2018) explore the topic and offer some confronting conclusions. Whilst any analysis such as these can be decried, the fact is the sentiments explored in these books are prevalent in large swaths of Western democratic societies, influencing the behaviours of many people to be focused on their view and wellbeing – potentially seeing themselves as victims - to the exclusion of them seeing themselves as part of a broader society.

Recognising the state of societal flux at the beginning of 2024 – war in the Middle East and Europe, nation-state competition including the threat of nuclear war, the tenets of globalisation and free market erosion, the challenging politics and economics of climate change, economic and personal financial stress – there is a need for people to act in concert for preservation. The reality is that people, as individuals, are historically empowered and more critical (and commensurately more vulnerable to misinformation), less tethered to societal pillars, more focused on their individual self and related discrete identity grouping rather than participating constructively in broader society of which they have diminished trust. How can we maintain the efficacy and effectiveness of society in the face of ever-increasing demands by individuals and tribes resulting in diminishing cohesion? How can we protect the effective operation of government and business for the benefit of the societies they serve?

Amongst the consequences of these changes in characterization of society, of change in societal mores,[6] are many individuals' diminished trust and loyalty in the institutions and leaders that have historically guided societies.

> *How far should leaders and managers be prepared to go, how accommodating should they be, to give comfort to changes in society, which promote asserted individual rights, at the potential expense of performance and security of their enterprise? In being so accommodating are they enabling insider threat in the enterprise?*

> [The] reduction in social coherence—or unity—contributes to fracture within our society and provides the space for insider threats to take root, to propagate, to succeed, and cause catastrophic damage.

Trust

A key element of the changes in society is the concept of trust.[7] In discussing insider threat, it is those who have legitimate access to an enterprise's assets and operations who are most relevant. Our current environment is comprised of people with diminished trust in the pillars of society. In the context of their lives, the 'who' and 'what' sources of information they trust are less predictable than in the past. There is a trend to refer to one's *lived experience*[8] of how these pillars have impacted one's life, rather than people holding a broader view of themselves as part of a society willing to rely on consuming and trusting information that others provide. This view repudiates empirical fact in favour of 'fact' being shaped by one's experience and perception – everyone is empowered to create their own 'facts'. The pillars they might have trusted to guide their thinking and inform their position are weakened or redundant leading to a deficit of trust in significant proportions of Western societies, and hence in our workplaces.

The *2023 Edelman Trust Barometer,* in its 23rd year of production, surveyed more than 32,000 people in 28 countries[9] in the period 1 – 28 November 2022. The theme for its 2023 report is *Navigating a Polarised World*, and in its Australia-focused analysis cites 'four forces that have Australia on the path to polarisation', those forces being:

- **Economic Anxieties –** Economic optimism is collapsing around the world, with 24 of 28 countries seeing all-time lows in the number of people who think their families will be better off in five years.
- **Institutional Imbalance –** Business is now the sole institution seen as competent and ethical; government is viewed as unethical and incompetent. Business is under pressure to step into the void left by government.
- **Mass-Class Divide –** People in the top quartile of income live in a different trust reality than those in the bottom quartile, with 20+ point gaps in Thailand, the United States, and Saudi Arabia.
- **The Battle for Truth –** A shared media environment has given way to echo chambers, making it harder to collaboratively solve problems. Media is not trusted, with especially low trust in social media.

Key points from the report include:

- Trust Index (the average percentage trust in NGOs, business, government and media) in a comparison between 2022 and 2023 reports saw Australia decrease trust (second worst result) whereas the U.S. had the biggest increase in trust.
- All Australian governments are distrusted.
- In Australia, business remains the only institution seen as competent and ethical.
- The key workforce demographics of Gen Z (born 1997-2012) distrust government and media with neutral levels of trust in business and NGOs.
- Millennials (born 1981 to 1996) distrust government and media and have neutral trust in business and NGOs.
- Institutional leaders are distrusted, with co-workers the most trusted.

For the Australia, United Kingdom, United States (AUKUS) security partners, with respect to global distrust threatening to polarise societies, Australia is assessed as moderately polarised. By comparison, the UK is assessed of being in danger of severe polarisation and the U.S. is assessed as now being severely polarised.

In exploring Australia's social fabric, 61% of Australian respondents cited 'the lack of civility and mutual respect is the worst I have ever seen' and 54% said that 'the social fabric that once held this country together has grown too weak to serve as a foundation for unity and common purpose'.

The report offers ideas to correct course in an increasingly polarised world by:

- **Supporting your home base –** The data has been very clear in the need for business to prioritise those in their own backyard by directly addressing their anxieties and working to reassure. It will be important to listen to your workforce to effectively drive change that is meaningful and impactful to the workforce.
- **Collaborating with government –** The best results come when business and government work together, not independently. Look for opportunities to build consensus and collaborate on policies and standards to deliver results that encourage a more just, secure, and thriving society.
- **Empower Gen Z –** It will be critical to better understand Gen Z as they engage with and value things very differently to those before them. Gen Z is driving a generational shift in trust which will be critical to address on the pathway to change, to set a new tone for the future.
- **Courage to take a stand –** A grim economic view is both a driver and outcome of polarisation that fuels distrust. Have the courage to take a stand on key issues that unify and hold divisive forces accountable.

This report describes a deteriorating society, a trust deficit, and indicates that people are looking for sources of trust – polarisation is not inevitable and may be reversible. People are more likely to trust business rather than government.

The challenge is to reconcile people's general lack of trust in the pillars of society, and their consequential move away from those in favour of a myriad of other societal groupings, and the opportunity for leaders and managers to capitalise on the workforce's willingness, even need, to trust the enterprise they are employed in.,

Turning to research[10] about trust, a long-term study investigating people's neurological responses to 'trust' concluded that building a culture of trust is what makes a meaningful difference to individuals relationship with work and hence to the enterprise they are part of. The research indicates that people in 'high-trust' enterprises are more productive, have more energy at work, collaborate better with colleagues, and stay with their employers longer. This high trust environment meets their needs as a person. The study offers eight management behaviours that can foster employee trust. The study offers that leaders and managers are the fundamental enabler to grow trust: leaders must provide the conditions for success – clear direction and suitable resources – then allow people to get on with the task, supervised (coached) but not micromanaged. I contend that a person is less likely to become an insider threat to an enterprise which offers them a culture of trust within which they are emotionally rewarded and socially enriched.

> *There is an opportunity for enterprises, especially private sector, to meet a fundamental employee need though creating a workplace culture based on knowing and communicating what the enterprise does and the contribution it makes to society. Culture of this type is likely to engender trust – to meet peoples' need to trust – as they feel a sense of supportive belonging which their tribe or broader society does not satisfy.*

Loyalty

Dr Kris Veenstra has written[11] on the topic of loyalty, social identity and insider threat. Whilst the research focused on suitability for employment in a high security government agency in the United States or Australia, in the context of insider threat and using Edward Snowden[12] as the exemplar the findings are relevant to any enterprise.

> Dr Veenstra writes: *According to social identity principles, the social identity an individual holds (i.e., self-definition's derived from group memberships such as their employing agency) play a significant role in the way they see themselves and how they behave. When people think of themselves in terms of a social identity, particularly if it is one that is valued and important to them, their individual interests become entwined with those of the group. As a result, they are more inclined to conform to group norms and demonstrate loyalty. Furthermore, loyalty is an outcome of the identification process. The more strongly someone identifies with their employing agency, the more loyal they will be.*[13]

The topic of social identity appears to be relevant to the 2023 case of U.S. citizen Jack Teixeira, alleged responsible for leaking of a significant trove of U.S. intelligence material, which is a case of insider threat because Teixeira's employment with the U.S. Air National Guard afforded him access to classified information. Reports that Teixeira posted classified material on a website, on which he was well known under a pseudonym, to generate notoriety amongst website users is of particular interest in terms of where his loyalties rest. It seems his loyalty rested with himself and his virtual activities rather than with the institutions and people who had offered him trust and loyalty in the 'real world'.

Recent reporting[14] about Jack Teixeira noted that members of Teixeira's chain of command have been charged over his theft and posting of classified information. The official investigation identified at least four instances of Teixeira accessing intelligence for which he had no legitimate access with supervisors being aware but not reporting it. Similar lacklustre management and leadership was evident in the Edward Snowden case with his supervisors not acting on, nor reporting, aberrant insider threat behaviour.

> **"...the value of human-based mitigations – leadership, culture, communications, employee support – and the ability of leaders to understand the operating context are indispensable mitigations to meet insider threat, a human-based threat.**

Snowden and Teixeira are for me, based on published information, emblematic of the person who becomes an insider threat: they made a decision to reject the trust and loyalty extended to them by a group they have sought to be part of and had been accepted into. Further, Snowden and Teixeira showcase technology as both the enabler of their thefts and the means to satisfy their personal agenda by using technology to promulgate the information they stole.

In the 20th century, loyalty was rooted in nationalism bound to national security through pain of war and so was seemingly straightforward to discern – society's institutions provided social identity. Our understanding of loyalty has moved from analogue to digital – it's more complex now.

Peoples' connection points for their loyalty have eroded in the same way as societal pillars have. The internet opened vast frontiers for new types of social identity – of connection points for loyalty – to be created. This diffusion of loyalty points has rendered the concept of loyalty increasingly complex and more difficult to assess.

Needs of the Many and the Needs of the Few

In the 1982, Star Trek film The Wrath of Khan, Spock says "Logic clearly dictates that the needs of the many outweigh the needs of the few." To which Kirk answers, "Or the one." This dialogue, steeped in utilitarianism,[15] has remained with me through the years as I have seen changes in society, enabled by technology and postmodernist thinking, swing the pendulum from mid-20th century 'big society' – the many – to cross the equilibrium to favour smaller groupings – the few – and it seems some have pushed the pendulum even further – to the one. That said, Kirk's answer signals recognition of instances where a compassionate response by society, recognising that there are instances to prioritise resources for people in absolute need, such as those with a physical disability, are homeless or suffering a mental health condition. The 'many' can selectively support the 'few', or the 'one'.

People (employees and contractors) are generally an enterprise's greatest asset. People are needed to deliver the product or service which is the reason the enterprise exists, and work as a team to achieve this. People, therefore, can be the greatest risk to the enterprise because they are trusted by the leadership and, in return, leaders seek peoples' trust and anticipate their loyal behaviour.

> *Leaders and managers must deliberately balance the needs of the many, the few, and the one. This issue is particularly relevant to insider threat as we navigate the friction between maintaining security and purpose of the enterprise versus observing individual employee preferences, always respecting employee rights in law.*

Countering Insider Threat

There is an imperative for managers and leaders to understand their responsibilities and legal obligations with respect to the enterprise they oversee. Enterprise security (against both internal and external threats) for the purpose of protecting the many takes precedence over a seemingly ever-expanding effort to mollify insurgent employees and external interest groups – the few. Malicious actors will take advantage of vulnerabilities arising from employee behaviours and employer insouciance.

Protecting the many, rather than ferreting out the few, may be criticised by some mangers, employees, and unions as potentially increasing the risk of insider threat. However, the alternative to not responding to the evolving insider threat is to suffer the consequences of vulnerabilities being exploited, resulting in materiel damage to an enterprise as demonstrated by Teixeira and Snowden.

Dr Eric Lang, in his *Seven (Science-Based) Commandments for Understanding and Countering Insider Threats*,[16] writes: "Without effective management, such insider threats can undermine mission execution, employee safety, productivity, morale, financial stability, network functioning, asset integrity, public welfare, and local and global trust." Amongst Dr Lang's seven commandments are some I see of particular relevance to this discussion (my observations in *italics*):

- **Human factors are paramount.** *Effective leaders appreciate the threats to their people and create relevant controls that identify risk events and assist their people to operate securely thus promoting the wellbeing of both employees and the enterprise.*

- **Employees are an organization's greatest strength, especially for identifying insider threats.** *Enterprises already invest heavily in recruitment, retention and support for their workforces. We can invest greater resource in protecting the workforce we've recruited, retained, and supported.*
- **Initial personnel screening is critical but not sufficient.** *The granting of employment should not be the end of the vetting and screening process. People change throughout their employment cycle; an ongoing assessment as part of an enabling security framework that safeguards both the employee and the enterprise is necessary.*
- **Leadership and organizational culture at every level are key.** *Leaders and managers need to appreciate the value and significance of the asset they are responsible for and are duty-bound to protect it. In taking action to protect the asset they are also protecting the wellbeing of the workforce in terms of a safe working environment, supportive culture and, in extreme situations, the ongoing existence of the asset and hence employment of the people dependent on their decision making. Culture is king and must be demonstrated by leaders and managers.*

Countering Insider Threat in a Fractious Workforce

How might leaders and managers counter insider threat in a contested environment where employee trust and loyalty are difficult to identify and win, social norms are eschewed in favour of self or tribe, victimhood is celebrated as part of social justice expectations and the pressures of day-to-day life can convert a trusted employee into a trusted insider overnight?

Based on our client engagements and research I offer the following observations to help counter insider threat.

- Insider threat is a perennial source of harm and is endemic in the workforce.
- Insider threat is consequential, irrespective of the nature of the insider threat, be it careless, negligent, malicious or coerced.[17]
- Robust legal pre-employment screening is essential. The pre-employment process is the best opportunity to mitigate insider threat because of the potential thoroughness of the process and the opportunity to determine a candidate's 'fit' with the culture and values of the enterprise. Getting 'fit' right is more important than employment skills as these can be taught.[18]
- Surveys highlight the vast majority of insider threat events are careless or negligent. Accordingly, targeted security education and employee support is a key mitigation to the largest part of the risk posed by insider threat.

- Culture is king. Because insider threat is about people, as distinct from a cyber threat or natural hazard threat, a people-centric approach (albeit supported by information technology) is required. Create an enterprise culture people want to be part of, a culture that they will want to trust and be loyal to.
- Leadership and clear messaging of expected behaviours are fundamental inputs to culture and human resource activity as the spine of all insider threat mitigation. Leaders and mangers need to be confident and equipped to act humanely and legally to perceived aberrant behaviours for the benefit of the many as well as for the benefit of the few. But they must act.
- Leaders need courage to make contentious or unpopular decisions, informed by a risk assessment, in the face of dynamic social norms and workforce expectations in order to mitigate insider threat.
- People are subject to drivers, some beyond their control. They may rapidly change to become an insider threat through no fault of their own and so there must be measures in place enabling timely detection of relevant indicators. Workplace colleagues are a key to timely detection, in concert with technical security means.

> *Insider threat is an ancient phenomenon but is a virulent and damaging threat today. Leaders and managers must actively counter insider threat to securely operate the asset or capability they are responsible for. Technical solutions are available as a mitigation, and should be used, however the value of human-based mitigations – leadership, culture, communications, employee support – and the ability of leaders to understand the operating context are indispensable mitigations to meet insider threat, a human-based threat.*

DISCLAIMER

The information and views expressed in this presentation are solely those of the author and do not represent opinions and policies of the Department of Defense, U.S. Government, U.S. Special Operations Command, the Joint Special Operations University, or the institutions with which the author is affiliated.

REFERENCES

1. H. Arendt, *The Human Condition*, University of Chicago Press, 1958.
2. Cambridge Dictionary definition: the act of treating someone as though they are not part of a group and are different in some way, 2023
3. H. Pluckrose and J. Lindsay, *Cynical Theories*, Pitchstone Publishing, North Carolina, 2020, p16 .
4. Standards Australia, *Handbook 167:2006 Security risk management*, jointly published by Standards Australia, Sydney, and Standards New Zealand, Wellington.
5. H. Pluckrose and J. Lindsay, *Cynical Theories*, Pitchstone Publishing, North Carolina, 2020, p17.
6. Mores are the moral beliefs, customs, and ideals that define acceptable, expected behaviour within a society or social group. Mores (pronounced "more-rays") are preferred and socially sanctioned ways of behaving in any given society. These are stronger forms of norms, in which more fundamental habits of behaviour are involved.
7. American Psychological Association, *APA Dictionary of Psychology*, Trust defined as: reliance on or confidence in the dependability of someone or something. In interpersonal relationships, trust refers to the confidence that a person or group of people has in the reliability of another person or group; specifically, it is the degree to which each party feels that they can depend on the other party to do what they say they will do. The key factor is not the intrinsic honesty of the other people but their predictability. Trust is considered by most psychologists to be a primary component in mature relationships with others, whether intimate, social, or therapeutic.
8. D. Chandler and R. Munday, *Dictionary of Media and Communications*, Oxford University Press, 2020.
9. Argentina, Australia, Brazil, Canada, China, Colombia, France, Germany, India, Indonesia, Ireland, Italy, Japan, Kenya, Malaysia, Mexico, Nigeria, Saudi Arabia, Singapore, South Africa, South Korea, Spain, Sweden, Thailand, The Netherlands, United Arab Emirates, United Kingdom, United States of America.
10. Paul J, Zak, *The Neuroscience of Trust: Management behaviours that foster employee engagement*, Harvard Business Review, January-February 2017 pages 84-90.
11. *K. Veenstra, Loyalty,* Social Identity and Insider Threat, for the Australian Criminal Intelligence Commission, November 2015
12. Edward Snowden was an American (now Russian) citizen who, whilst a contractor undertaking ICT-based tasking at the National Security Agency (NSA), stole millions of classified files which in 2013 he released either publicly or reportedly passed to Russia and China. Snowden accessed the classified files using the log on credentials of up to 25 NSA colleagues who gave their credentials to him. M. Hosenball and W. Strobel, Reuters 8 November 2013.
13. K. Veenstra, *Loyalty, Social Identity and Insider Threat*, for the Australian Criminal Intelligence Commission, November 2015, p5.
14. M. Myers, 15 *Air National Guardsmen disciplined in Discord server leak*, Military Times, 21 December 2023.
15. Utilitarianism promotes 'the greatest amount of good for the greatest number of people'.
16. Eric L. Lang, *Seven (Science-Based) Commandments for Understanding and Countering Insider Threats*, Counter-Insider Threat Research and Practice, Office of People Analytics, Personnel and Security Research Center (PERSEREC) 2022, page 1.
17. From the Institute for Critical Infrastructure Technology (2017), cited by Eric L. Lang, *Seven (Science-Based) Commandments for Understanding and Countering Insider Threats*, Counter-Insider Threat Research and Practice, Office of People Analytics, Personnel and Security Research Center (PERSEREC) 2022, page 2.
18. J. Kerr, *Legacy: What the All Blacks Can Teach Us About the Business of Life*, Constable, 2013.

ORIGINAL RESEARCH

The New Insider Threat: How Commercially Available Data can be used to Target and Persuade

Jaclyn Fox

Introduction

By day, 21-year-old Jack Teixeira was a Massachusetts Air National Guard Member working on IT issues at Otis Air National Guard Base (Lamothe and Harris 2023). By night, he was the moderator of a racist, misogynistic, antisemitic Discord server threatening mass violence against marginalized communities and law enforcement officials (Harris and Oakford 2023). Notably, these two lives were not completely separate; on base, Teixeira's colleagues feared that he was showing signs of becoming a mass shooter (Lamothe and Harris 2023). However, when the airman was finally arrested it was for another form of insider threat: classified leaks.

1 Beginning in February 2022 and continuing until his arrest in April of 2023, Teixeira would leak hundreds of classified documents onto two Discord servers, amounting to one of the largest intelligence breaches in decades (Harris and Oakford 2023). Although Teixeira leaked documents that interested him – such as classified information about the Ukraine/Russia war, he also took requests from anonymous individuals within the server. For over a year Teixeira evaded detection despite numerous warning signs; on at least three separate occasions Teixeira's supervisors saw him looking at classified materials outside the scope of his position (Harris and Oakford 2023) and his colleagues repeatedly raised the alarm about disturbing behavior and fetishization of violence. Ultimately, however, the leaks were only discovered after another individual re-posted the materials which led to their spread across the internet.

JACLYN FOX

Dr. Jaclyn Fox is a postdoctoral fellow with the Army Educational Outreach Program (AEOP) affiliated with West Point's ACI. She obtained her PhD in international relations from American University where her dissertation focused on the spread of extremist narratives and mis/disinformation online and its relationship to actions offline. At West Point, she is continuing this stream of research along with an increased emphasis on the issues of insider threat and privacy.

This particular form of espionage may have been surprising to Teixeira's colleagues who witnessed his violent and erratic behaviors, however, indicators available in Teixeira's *online* life warned of this threat. Although not tracked by the U.S. military, servicemembers' online lives paint an intimate picture of their psyches. If an external actor is able to gain access to insiders' online lives this could render U.S. servicemembers and the U.S. military vulnerable to manipulation. In today's world access to this kind of data is unfortunately not a matter of "if" but "when" as commercial data brokers are already working to aggregate individuals' online rhetoric and offline behaviors to make inferences about their personalities, mental health, and ideological alignment, for targeting as consumers.

While existing literature examines the factors correlated with the perpetration of insider threat (Allen et al. 2023; Herbig 2017; Greitzer and Hohimer 2011; T. J. Thompson 2018; 2014; Shaw and Sellers 2015; Lenzenweger and Shaw 2022; Bedford and Van Der Laan 2021; Hugl 2010; Wilder 2017), it does not discuss how the newest element of technological innovation – mass commercial data collection – can be leveraged by actors seeking to undermine U.S. national security interests.[2] The current paper seeks to fill this gap asking: is it possible to use commercially available data to cultivate potential insider threats?

To understand the potential for using commercially available data in this manner, we develop a framework of "insider threat" correlates and motivations based on the available empirical literature. We then search the commercially available data for potential proxy variables that measure these factors.

2 Of note, a recent study by Duke examined the issue of commercial data collection and the U.S. military specifically; however, their findings were limited both in number of brokers and breadth of audience segments discussed (Sherman et al. 2023). We build on their important findings. Our analysis is essential as audience segments not originally scoped for U.S. military personnel may be cross-referenced or geo-located to military spaces allowing for a much wider range of "military" data available..

For this project, the commercial data utilized comes from a dataset aggregated by Microsoft's ad platform, Xandr, that was exposed during a recent investigation by the Markup. This comprehensive dataset contains 650,000 "audience segments" across 93 different data brokers highlighting the depth and breadth of commercial data collection activities (Keegan and Eastwood 2023).[3]

From our analysis we found that it is indeed possible to use commercially available audience segments to cultivate a list of individuals with the predispositions, recent life stressors, and insider access[4] making them vulnerable to engaging in acts against their organization. In other words, our findings suggest that available commercial data can be weaponized by external actors to sow discord within the U.S. armed forces and to cultivate a list of insiders with the predispositions and life stressors making them vulnerable to engaging in actions against their organizations. Importantly, nefarious outsiders in this instance are not limited to state actors or those with extensive funding. Rather, the cheap nature of this data (Sherman et al. 2023)[5] allows for nearly anyone with a credit-card – located across the globe – to weaponize this intimate knowledge about our nation's insiders.

Literature Review

Due to the immense risk posed by individuals with insider access turning against their organization, multiple studies have aimed to proactively identify those likely to engage in insider threat. This includes in-depth literature reviews highlighting the traits common to insider threats, empirical studies, analysis of specific cases, and even modelling[6] (Allen et al. 2023; Lenzenweger and Shaw 2022; Bedford and Van Der Laan 2021; Whitty 2021; Shaw and Sellers 2015; Philip Legg et al. 2013; Greitzer and Hohimer 2011). While the literature focuses on different aspects of this problem, there is wide agreement that behavioral and psychosocial indicators are essential to understanding who might engage in acts against their organization. Importantly, this body of literature is written with the idea in mind that organizations have access to these variables in order to model threat within their workers; however, in this paper we seek to understand if the same datapoints could be captured within the available commercial data and instrumentalized by external actors with mal intent.

3 See previuos note .

4 Numerous audience segments are available that both directly and through proxies identify individuals in the U.S. armed forces and working in the government.

5 A recent study by Duke researchers (2023) found that individually identifiable information on U.S. servicemembers and their families could be purchased for as little as $0.12 a record. At higher quantities of servicemembers the cost dropped to $0.01 per individual (Sherman et al. 2023).

6 Various researchers have worked to model potential insider threats using the datapoints discussed above (see: Allen et al. 2023 for a review). For organizations, managers often have access not only to technical details such as what an employee does online but their behavioral indicators as well when brought to the attention of HR departments. One such model used interviews with HR professionals to pinpoint various indicators that one may engage in insider threat behavior. These behaviors are joined with network monitoring to create an algorithm that may identify potential threats..

Who Engages in Insider Threat? Psychological Factors/Psychosocial Factors

The first category implicated in insider threat participation is psychological and social factors. Based on extensive empirical research, psychological factors such as the "big 5," e.g. agreeableness, conscientiousness, neuroticism, and "dark triad traits," i.e. narcissism, psychopathy, and Machiavellianism, are key to understanding those with the potential to engage in insider threat. Specific characteristics have also been implicated in these activities including anger, frustration, social isolation, entitlement, and lack of empathy (Allen et al. 2023; Shaw and Sellers 2015; Greitzer and Hohimer 2011; Hugl 2010). Of note, while all of these traits have been named in the literature, some may be more influential than others; Greitzer and Hohimer (2011) for instance proposed a weighting scheme in their model with items like disgruntlement and anger management weighing more heavily than items like absenteeism in predicting the potential for insider threat (Greitzer and Hohimer 2011, 32). On the psychosocial end, addiction and mental health disorders have also been associated with the perpetration of insider threat; however, it's essential not to stigmatize individuals for merely having a disorder. Rather, mental illness may be one data point that in conjunction with other data points highlights the need for further examination of an individual.

While many of the available studies speak of "insider threats" broadly, Allen et al. (2023) divide the group categorically into espionage/mass leaking, counterproductive work behaviors, and workplace violence. This delineation is especially useful as it allows for the discussion of psychological and psychosocial correlates both overall and in relation to specific threat types. Spies overall tend to be narcissistic, thrill seeking, grandiose, and desire both power and control (Allen et al. 2023; T. J. Thompson 2014; Wilder 2017). However, Allen et al. (2023) expose a slight demarcation between those who engage in traditional forms of espionage (e.g. Robert Hanssen) and mass leaking (e.g. Edward Snowden). While both tend to display narcissistic traits, the former also tends towards psychopathy and immaturity while the latter displays a grandiose need for recognition, belief that they are performing a "greater good", personal convictions, and disgruntlement (Allen et al. 2023, 21; T. J. Thompson 2018; Herbig 2017; T. J. Thompson 2014; Wilder 2017). In terms of workplace violence – such as the attack on Ft. Hood by Nidal Hasan, research specifies the role of a *narcissistic injury* (White 2021).

Regarding counterproductive work behaviors, dark triad traits are also implicated (Ellen et al. 2021; O'Boyle et al. 2012) as are the "big 5" attributes such as low agreeableness, low conscientiousness, and low emotional intelligence (Bowling et al. 2011; Ellen et al. 2021; Zhou, Meier, and Spector 2014). Lastly, high levels of aggression are also correlated with perpetration of counterproductive work behaviors (Galić and Ružojčić 2017; Kranefeld and Blickle 2022; Runge et al. 2020).

> **If an external actor is able to gain access to insiders' online lives this could render U.S. servicemembers and the U.S. military vulnerable to manipulation**

Finally, we turn to workplace violence. As workplace violence is a type of insider threat, it shares potential indicators with other forms including espionage. These indicators include aggression, feelings of injustice, perceived wrongdoing of organization, social isolation, financial issues, and grievances (Department of Homeland Security 2019). However, workplace violence has additional indicators relevant to the perpetration of mass violence more generally that may differ from other forms of insider threat. These could include access to and skill with weapons, substance abuse, suicidality/depression, homicidal fantasies, and specific preattack planning and preparation (Viñas-Racionero, Scalora, and Cawood 2021; Cybersecurity and Infrastructure Security Agency (CISA) 2020; Occupational Safety and Health Administration (OSHA) 2016). Of note, individuals like Teixeira demonstrate the interrelated nature of different forms of insider threat; although Teixeria maintained weapons and threatened violence he ended up betraying his service through mass classified leaks. Indicators such as narcissism and grievance against the government highlighted Teixeira's vulnerability to engaging in acts against the government broadly even if they didn't point to the specific type of threat.

In sum, all variations of insider threat tend to correlate with some form of dark triad trait (especially narcissism), elements of the big 5 personality inventory, and aggression. However, predispositions alone do not lead to engagement with insider threat behaviors; rather, these behaviors may intersect with underlying grievances and specific triggering events culminating in acts against one's organization. Below, we discuss this important interaction.

Stressors: Who Engages in Insider Threats?

Within every segment of the insider threat paradigm, underlying grievances and recent life stressors are highlighted. That is, it is not predispositions alone that make an individual engage in acts against their organization but predispositions in conjunction with life stressors. Stressors can include work-related issues – such as a poor person/organization fit, a "moral qualm" with one's organization, recent demotions or bad performance reviews (Hugl 2010, 96). Stressors could also be in one's personal life such as a recent divorce or high debt (Shaw and Sellers 2015). These "critical triggering events" interact with grievance and personal predispositions to raise the likelihood

of an individual's decision to turn against their organization (Shaw and Sellers 2015; Wilder 2017; Herbig 2017; Allen et al. 2023).

Of note, the U.S. military recognizes the role that life stressors play in the potential to engage in insider threat. To combat this, the Office of the Director of National Intelligence has initiated a process of continuous evaluation in which public records are constantly scanned to proactively identify potential stressors including arrest reports, credit scores, bankruptcies, and divorce (Marks 2014).[7]

Motivations: Who Engages in Insider Threat?

In addition to predispositions and stressors individuals must have a motivation for engaging in insider threat behaviors. For individuals who ultimately decide to act against their organization, motivations can be categorized in three ways: economic, ideological, and disgruntlement/revenge (Allen et al. 2023, 21). However, these categories are not mutually exclusive; rather individuals are often driven by multiple impulses. Robert Hanssen, for instance, claimed that he was driven to spy for Moscow based on financial incentives; however, he also "burned with resentment that he did not receive the respect and assignments he felt he deserved" (Baker 2023). Mass leakers, on the other hand, the newest form of insider threat – and the one most quickly growing – tend to be driven by notions of "fairness" or "what's right." They enjoy playing the expert and see themselves as helping (Allen et al. 2023, 21). This is an especially interesting finding and supports earlier research that many insiders are not approached by external actors but rather are driven to volunteer their services (Irvin and Charney 2014). New technology then may act to facilitate this underlying impulse as opposed to the number of individuals wishing to engage in this behavior actually increasing.

7 This is intended to be a supplement to security clearance investigations which occur every 5-10 years.

Of note, although neither financial nor ideological motivations are generally the sole motivating factor for involvement in insider threat actions (T. J. Thompson 2014; Allen et al. 2023, 22), finding proxies for both financial stress (e.g. large debts, bankruptcies, or gambling) and ideological positions (including moral qualms with organization) (T. J. Thompson 2018) in the commercial data would be useful to identify potentially vulnerable insiders. In the case of ideology for insider threat in the military, this could include proxies for trust in government, alignment with certain ideological positions (e.g. LGBTQ+ rights), or political alignment (especially if this is in opposition to the party in power).[8]

The last category of motivation revolves around disgruntlement/revenge against one's organization. This could take a multitude of forms including: viewing work as illegitimate or above one's pay grade, job insecurity, perception of poor person/organization fit, perceived injustices at work, unfair pay, or "psychological contract breaches" (Zhao et al. 2022; Berry, Ones, and Sackett 2007; Liao et al. 2021; Mackey et al. 2017; Allen et al. 2023). Some of these work-related grievances — such as poor person/organization fit — may also be elucidated through the ideological proxies discussed above.

As a final note, although the literature on insider threat pulls from different fields, including cyber security, information sciences, and behavioral sciences, different organization types (e.g. private sector vs military) and utilizes different methodologies, there is general agreement in the variables of interest for detecting potential insider threats. To detect potential threats one must look at individuals' predispositions – including psychological and psychosocial factors – stressful life events, and issues with the organization itself such as perceived ethical alignment (Hugl 2010, 94; Shaw and Sellers 2015; Greitzer and Hohimer 2011). It is these traits that we will focus on in the current study and aim to identify in the commercially available data.

As discussed, the key question for the current study is, would it be possible for an external actor to use commercially available data to cultivate a list of individuals with insider access who may be more likely to turn against their organization? The available literature paves the way for this process, allowing one to create a "framework" for insider threat perpetration and determining which variables one would look for in the data itself. However, before discussing the creation of this framework and its application, it is worthwhile to highlight the recent research on commercially available data more broadly.

Commercially Available Data

Recent research has implicated commercially available data in a variety of destructive

8 In terms of *violent* insiders, although ideological extremism may be present, radical beliefs are not sufficient for engagement with violence (e.g. Asal, Schulzke, and Pate 2014; McCauley and Moskalenko 2017). However, radical beliefs may shape the form the violence takes place in – such as the target choice (Allen et al. 2023).

outcomes for individuals. This includes reports of data brokers selling data of elderly people and those who are believed to be in cognitive decline so that they can be targeted with fraudulent content (Simmons and Sherman 2022) as well as a report by the Cyber Policy Program at Duke University revealing that data brokers advertise their lists of veterans and U.S. military personnel (Sherman 2021). Finally, research has pointed to numerous real-world implications of commercial data collection including people being denied medication (Szalavitz 2021), rejected for rental applications and home loans (Johnson 2023), or facing increasing barriers to government services (Donnan and Bass 2022).

In terms of military operations specifically, researchers at the Army Cyber Institute have recently begun digging into the commercial surveillance landscape in efforts to better understand what is revealed through commercial data collection. Investigative reports like those published at the Intercept, show detailed location identification through companies like Anomaly Six that can identify where specific individuals regularly visit and live (Biddle and Poulson 2022). Others, show how easy it is to dig deep into the data of millions of cell phones and identify a single military user or reveal nuclear secrets through online flashcard apps (S. A. Thompson and Warzel 2019; Postma 2021). Further reporting revealed the location of forward operating bases in remote areas through fitness apps like Strava (Hsu 2018). Finally, the battlefield in Ukraine is also revealing just how dangerous commercial devices are on the battlefield. The Russian military allegedly banned smartphone use by its soldiers back in 2019 (Nechepurenko 2019). This is an important development as Ukrainian forces are using social media posts to locate and attack Russian military and paramilitary forces (Burgess 2022).

While the above emphasizes the damage that commercial data collection can cause, it is worth discussing a few key points about data brokers *themselves* to better contextualize risk for the current study. The first point is the low-cost nature of this highly sensitive personally identifiable data. The Duke study, referenced above, showcased not only the ease of acquiring mass amounts of personally identifiable information but its cost-efficiency (Sherman et al. 2023). Posing as buyers from both the U.S. and Asia they were able to purchase bulk sensitive data on U.S. servicemembers and their families including health data, financial data, marital status, political affiliation, religious affiliation, children in home and interest in gambling for as little as $0.12 a record (Sherman et al. 2023, 29, 33, 37).[9] Further, the researchers were able to make these purchases without any verification of their identity.[10] This means that individuals with

9 The authors note that the cost per service member they were quoted ranged from $0.12 to $0.32 depending on how many records were being purchased at a time and the selection of variables. However, in greater numbers the per individual rate can drop to $0.01. Persistent location information was also available although the team did not purchase this.

10 Of note, verification practices varied by broker. However, for the ones that did verify buyer's identity, the process appeared to be about ensuring payment as opposed to risks posed by the sale (Sherman et al. 2023, 26). Further, one broker said that they required identity verification, but relented if the purchase was made by wire as opposed to credit card (Sherman et al. 2023, 26).

nefarious intentions, including foreign adversaries, or violent extremist groups, can easily purchase large quantities of personal information related to U.S. servicemembers and their families for blackmail, manipulation, or, as highlighted in the current study, to develop their own "insiders."

Additionally, even if brokers refuse certain entities – like foreign adversaries – the ability to purchase bulk sensitive data, the data itself is often perilously easy to hack or intercept. Recent high profile data hacks, such as Equifax and Marriott have demonstrated both this possibility as well as the interest (Del Valle 2024; Liptak 2018; Warren 2018). Further, researchers have showcased how a skilled individual could intercept sensitive information while it is being transmitted to data brokers from the apps that collect it. A report from the Consumer Council of Norway (2020) found that even the most sensitive information, like GPS coordinates, was being transmitted to data brokers from the apps in which it is collected on unencrypted connections, posing a serious security threat (Forbrukerrådet 2020, 103). That is, not only are apps *selling* (and sharing) users' sensitive data to brokers who aggregate and resell it, but the manner in which they 1) store this information[11] and 2) transmit it is so insecure that external actors can easily intercept the personal information.[12]

In the next section we lay out the research design for the current study, building on previous literature on commercial data collection as well as insider threat broadly, by mapping the potential for commercial data to be used to detect and exploit insider threats. We begin with a discussion of The Markup's investigation, followed by an analysis of the commercially available audience segments.[13]

> **Predispositions alone do not lead to engagement with insider threat behaviors; rather, these behaviors may intersect with underlying grievances and specific triggering events culminating in acts against one's organization.**

11 Dating apps in particular are a wealth of personal information including: persistent location, sexual orientation, religious affiliation, political ties, and drug use which have consistently been shown to lack appropriate data protections. Not only is the data sold to third parties but Tinder, Bumble, OkCupid, Grindr, and Facebook dating have all reported breaches (Rizvi and Fern 2021). In 2018, Grindr's data was breached exposing incredibly sensitive personal data including HIV status and GPS data – even if the user had proactively opted out of sharing the latter information (Ikeda 2020). While Grindr claimed to have solved the issue a follow-up report in 2019 found that this was not the case (Ikeda 2020).

12 Cybersecurity experts have also demonstrated the ease with which an external actor could pinpoint an individual's precise location by using trileration attacks on apps such as Tinder and Grindr. While Tinder reportedly fixed this error, Grindr was still vulnerable in follow-ups in 2016, 2018, and 2019 (Koch 2024; Ikeda 2020).

13 See https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you for the Markup's investigation.

Research Design

The purpose of the current study is to understand the depth and breadth of commercially available data being captured on individuals with insider access. Due to the wide-ranging nature of this data we focus on the key question: does data exist that would allow a nefarious outsider to identify individuals with classified access who may have the predispositions, recent life stressors, and motivation to engage in actions against their organization?

In June of 2023, researchers from The Markup uncovered a spreadsheet labelled "Data Marketplace – Buyer Overview" on the website of Microsoft's ad platform Xandr (formerly owned by AT&T). This database contained over 650,000 audience segments[9] across 93 data brokers and illustrates the troves of personal data being collected on individuals (Keegan and Eastwood 2023). For the current study, we analyzed the contents of this database with respect to identifying potential insider threats. The top 10 data brokers within the Xandr database are listed in Table 1.

Within the database, audience segments ranged from the mundane to the mortifying. Advertisers could target based on demographics such as location, relationship status, and age/sex as well as more sensitive topics such as the investigation's titular "heavy buyers of pregnancy tests." Additionally, advertisers could target lists of consumers based on psychological profiles such as the big 5 personality traits, reactivity to stress, and thrill-seeking behaviors as well as those working in the U.S. military or government. This data will prove key to identifying potential insider threats.

Table 1. Top 10 Data Brokers

Data Provider Name	n
Audiences by Oracle (BlueKai, Datalogix, AddThis)	132645
LiveRamp Data Store	82363
Grapeshot	73569
Nielsen Marketing Cloud	65610
Eyeota	53526
Factual Inc (Foursquare, location data)	29208
Oracle Customs (1st, BlueKai, Datalogix, AddThis)	26288
Adsquare (Data Provider)	15246
Dstillery	12630
Skydeo, Inc.	11972

**Note, data brokers are not synonymous with data providers. For instance, Experian is a very large data provider, however it is sold through brokers such as Oracle Customs and KBM Group.*

While consumers may have a vague notion as to the possibilities of data collection – phones' location data providing a timeline of places travelled, purchases made on credit cards aggregated, most are likely unaware of the scale of this collection, the ways in which it becomes tied together, or the ability of companies to use various pieces of information to create algorithms that make inferences about individuals including psychological profiling of personality traits.

14 An audience segment can be understood as a grouping of individuals for the purpose of targeted advertisement. Some of these segments are familiar and seemingly benign, e.g. individuals between 18 and 29, while others highlight the intimate details being collected on individuals. These could include individuals with specific mental health diagnoses, those who have insomnia due to chronic pain, and those who are caregivers for children.

Data and Methods

For the current study we wanted to understand the potential for misuse of the Xandr dataset by a nefarious actor. The research is guided by the question:

> **Can commercially available data be used to cultivate a list of potential insider threats for targeting?**

To investigate this possibility, we analyzed the dataset looking for the predispositions, life stressors, and motivations for engaging in insider threat behavior based on our literature review. When these factors are crossed with audience segments denoting individuals working for the U.S. military or government[15] this can create a list of potentially vulnerable individuals with insider access. While the available literature focuses on modeling potential insider threats for organizational security, we posit that these same characteristics can be used to reverse engineer a list of individuals with insider access who may be most vulnerable to engaging in actions against their organization. Thus, we were interested in whether the data could be used to identify relevant:

1. **Predispositions (e.g. psychological and psychosocial)**
2. **Life Stressors (e.g. divorce, financial stress)**
3. **Motivations (e.g. financial, ideological, work related)**

15 Numerous audience segments are available that both directly and through proxies identify individuals in the U.S. armed forces and working in the government.

Searching the Dataset

We began by developing a list of variables relevant to each of the above categories based on the literature review. For the psychological variables, for example, we created a list that included items such as "narcissism," "psychopathy," "thrill seeking," "conscientiousness," and "agreeableness." While some variables, such as "thrill seeking" had explicit audience segments in the dataset, others, such as narcissism, did not. We therefore expanded our search in two ways: word-based searches looking for synonyms that captured the same concept and broker-wide pulls on data brokers that were identified to capture other traits of interest.

In other words, we performed word-based searches of the Xandr dataset for 1) exact wording corresponding to specific variables implicated in the literature review, e.g. "narcissism" and 2) synonyms/related concepts to the identified variables, e.g. "self-involved". We then pulled all audience segments belonging to brokers that were identified as trafficking in any of the insider threat variables based on the initial word searches.

In this way, for each variable implicated in the literature, we searched for:

1. an **explicitly named audience segment,**
2. an **implicitly named audience segment** (i.e. named in an intuitive way that the researchers proactively searched for), and
3. an **audience segment covering the concept named in an idiosyncratic way** that did not appear in word-based searches but was sold by the same data broker trafficking in other segments of interest.

Table 2 outlines the key variables we sought in our analysis and relates them to the literature on insider threat perpetration.

Table 2. Insider Threat Framework

Category from Literature	Sub-Category from Literature	Exemplar Variables Sought from Database
Predispositions	Personality	• Dark Triad • Big 5 • Other Traits of Interest, e.g. anger, thrill seeking
	Psychosocial Traits	• Substance Abuse • Mental Health
	Demographics	• Gun Ownership
Stressors	Family	• Marriage/Divorce • Pregnancy • Terminal Illness • Recent Death • Frequent Moving
	Work	• Low Job Satisfaction • Moral Qualm with organization
Motivations	Financial	• Loans • Debt • Bankruptcy • Financial Changes • Gambling
	Ideological	• Immigration • LGBTQ+ • Abortion • Guns • Conspiracy • Trust in Institutions (media, banks, govt, social media) • Political Alignment
	Disgruntlement/ Revenge Against Organization	• Disengaged Worker • Overqualified Worker • Low Job Satisfaction • Ideological Misalignment with Organization (e.g. moral qualm)

> **For a small sum of money, external actors can purchase this dataset, allowing them to target thousands of potential insider threats.**

Ultimately, we developed an "insider threat framework" modeled off of the literature that seeks to proactively identify individuals who may engage in actions against their organization. The framework contains predispositions, stressors, and motivations for engaging in insider threat implicated in the empirical research.

Results

Our results show that the available commercial data can be used to identify individuals with insider access who may be more vulnerable to engaging in actions against their organizations. In fact, *all* of the data points from the Insider Threat framework in Table 2 are available for purchase from various data brokers. Below, we highlight key examples of available data by insider threat category; **Table 3 in the appendix lists exemplar data points for each framework item**.

Predispositions: Personality

As noted in the literature review, personality factors are a key correlate for willingness to engage in insider threat. From the available variables one could attain rough psychological profiles of current and former military members, cultivating lists of those with relevant (i.e., correlated with insider threat perpetration) traits. This has the potential to be a remarkably powerful – and low cost – way to target those with classified access who may be most likely to turn against their organization.

For example, the big 5 attributes, such as agreeableness (low), neuroticism (high), openness (low) and conscientiousness (low) are heavily implicated in the research on insider threat. All of these audience segments are available for purchase and can be cross-referenced with military members leading to a cohort of individuals with personality vulnerabilities and insider access.

VisualDNA Personality – US – Agreeableness – Lone Wolves

VisualDNA Personality – Personality – Agreeableness – Disinterested

VisualDNA Personality – US – Neuroticism – Trapped

Elements of the "dark triad" (i.e. narcissism, psychopathy, and Machiavellianism) are also linked to insider threat. Although these traits are not searchable within the commercial data directly, available audience segments (such as those listed below) can serve as proxies.

VisualDNA Mobile & App > Personality > UK > Agreeableness > Self Focused

VisualDNA Personality – Personality – Agreeableness – Control Seekers

Eyeota – US Experian – Psychographic / Attitudes – Self Concept – Dominating / Authoritarian

Eyeota – FI NDR – Insight360 – Values360 – 2 Self-centered and passive

Additionally, proxy variables can be found for anger/rage, poor stress tolerance, engagement with risky behavior/thrill seekers, and those with untapped grievances.

VisualDNA Personality – US – Neuroticism – Stress Reactors

VisualDNA > Personality > US > State of Mind > Frustrated

Eyeota – US Experian – Psychographic / Attitudes – Personal Views – Social Isolation

Eyeota – AU RDA Research – Consumer Profiles – Demo – General Attitudes – I generally get a raw deal out of life

Branded Data > Audigent > Programmatic Audio > Interest and Affinity > Thrill Seekers (BlueKai)

It is worth noting that just because individuals have this collection of traits, that does not mean that they will engage in insider threat behavior. As such, these categorizations should not be used to penalize individuals who are otherwise performing their duties. However, an adversary with access to a list of these individuals and malign intent could potentially cultivate insiders willing to turn against their organization.

Psychosocial Traits and Demographics

In addition to the psychological traits highlighted above, audience segments also illustrate individuals with demographics and psychosocial aspects that may increase their vulnerability to engaging in insider threat. Substance abuse has been implicated repeatedly in cases where individuals act against their organization, particularly with workplace violence. In addition, access to weapons is a key factor for individuals who go on to commit violence against their organization (Department of Homeland Security 2019). Exemplar segments are listed below.

Neustar AdAdvisor > AdAdvisor Political Audiences > Outlook > Gun Owners

Clickagy > Health > Addictions > Drugs

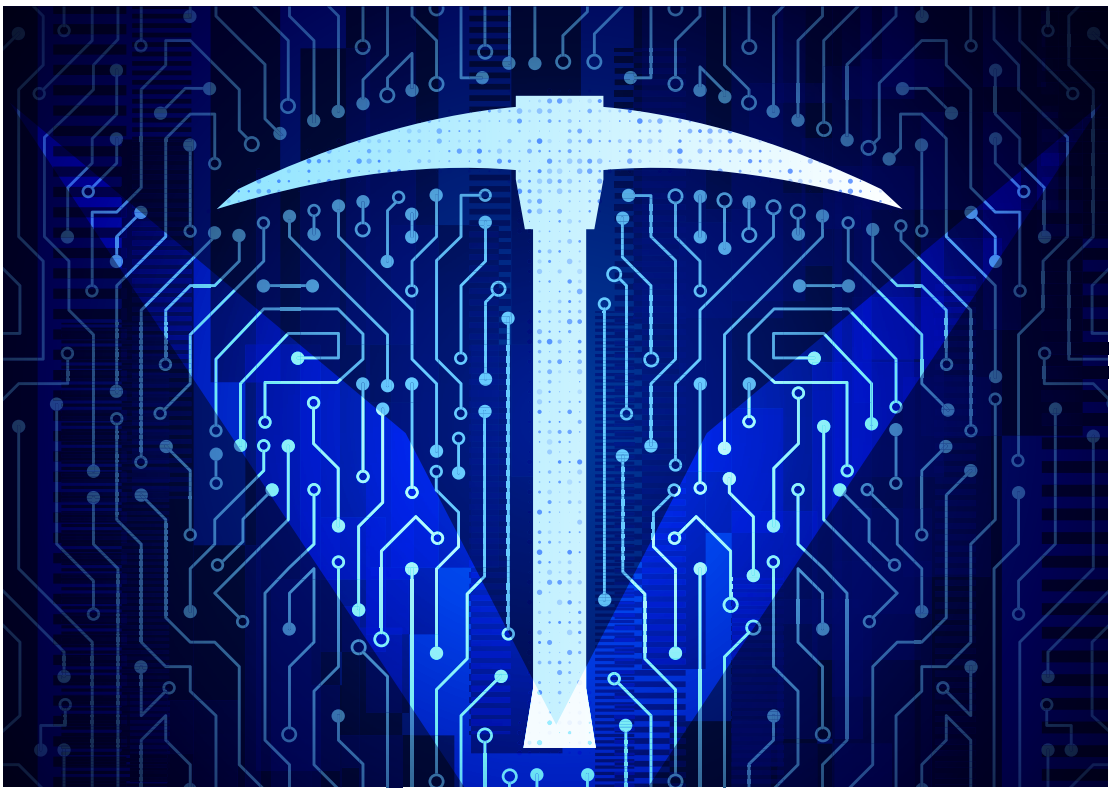
Skydeo > ConditionGraph > Health & Wellness > Lifestyle Indicators > Alcohol: Drink & Drive

Further, the data allows targeting of individuals with specific mental health diagnoses, such as PTSD, Anxiety, Depression, and Bipolar disorder. In addition, it highlights individuals who have been prescribed medication to treat these mental illnesses. It's important to note that mental health diagnoses in and of themselves do *not* indicate an increased propensity to engage in insider threat. It is thus important not to malign individuals with any mental health diagnosis or treatment. However, certain mental illnesses (such as those listed below) have been correlated with insider threat in the presence of additional factors. Additionally, if individuals use telemedicine or have their medications delivered by mail (both available audience segments) this could potentially open them up for tampering by malign actors.

Disease Propensity by Type > Anxiety Diagnosis (Adstra)

Eyeota – US Kantar – Health and Wellness – Conditions and Treatments – Post Traumatic Stress Disorder or Ptsd

Kantar > US > Custom > Use Any Rx Treatment for Depression



Stressors

After accounting for psychological and psychosocial predispositions and demographic characteristics, the next most important aspect of vulnerability to engaging in insider threat is experiencing recent life stressors. Research on previous cases of insider threat, in particular espionage, reveal individuals experiencing both professional and personal life stressors including "moral qualms" with their organization, financial difficulties, problems at home, and interpersonal issues at work. Reality Winner, for example, a former NSA contractor who leaked classified material to the online publication The Intercept, revealed moral qualms she was having both during her time in the Air Force and then at the NSA. In her home life, Winner experienced a major personal stressor right before leaking, losing her father with whom she had a close (but complicated) relationship (Stack 2022).

Audience segments are available to capture these varying personal and professional stressors including recent death, terminal diagnoses, those newly divorced, separated, married, or single, and those who feel disconnected from their work environment.

Adyoulikesa_bereavement

Consumer > Healthcare > Healthcare – Terminal Illness & Counseling

Branded Data > Media Source > Demographic > Family Composition > Marital Status > Recent Divorce (BlueKai)

Branded Data > Experian > Life Event > Recently Married > Last 3 Months (BlueKai)

Predictive Audience > Eyeota > Demo > US – Life Events – Expectant Mothers / Pregnancy

Skydeo > ConditionGraph > Health & Wellness > Job Satisfaction > Low Job Satisfaction

Motivations

In addition to *who* may be most vulnerable to engaging in insider threat actions, the commercially available data allows one to understand *why* these individuals would be willing to turn against their organizations. That is, audience segments are available for each of the three key categories of insider threat motivation: economic, ideological, and disgruntlement/revenge. These categories are not mutually exclusive; economic motivations, for instance, are often present but not the sole motivating factor for individuals who work against their organization (Allen et al. 2023, 22). Through the available data, however, one can ascertain which individuals may be motivated due to financial, ideological, or revenge-seeking needs.

Financials

Individuals with financial motivations to engage in insider threat can be ascertained through audience segments containing individuals with large loans, significant debt, gambling habits, and bankruptcies. Perhaps even more relevant are those with *recent financial changes* which includes individuals who saw their disposable income decrease by over 75% in the last 5 years. Although it is not clear how much these individuals still have, the perceived relative deprivation could be a major financial motivator. Essentially, a malign actor could target individuals involved in military or government work who hold large debts, are gambling addicts, or are seeking immediate loans and offer a way out of their financial struggles.

Ideological

A second category of motivation to engage in insider threat is related to ideological beliefs. Within the commercial data there are audience segments that target individuals on both sides of contentious issues including: abortion (pro-life/pro-choice), support for gun control vs support for the 2nd amendment, immigration issues, views on the LGBTQ+ community, and others. These ideological buckets serve the dual purpose of identifying individuals with an ideological motive for "revenge" against an organization as well as formulating potential targets lists. Audience segments also capture those who support conspiratorial and anti-government views and individuals' overall political alignment.

Targeting individuals who consume conspiratorial media or those who self-identify as doomsday preppers and "patriots seeking security" — all available audience segments — would be especially useful in the case of insider threat within the military or government. In addition, targeting individuals by support for (or rejection of) politicians like former President Trump could identify those with military/government related ideological grievance.

In sum, ideological audience segments can be utilized to identify individuals who may be anti-government (e.g., self-designated "patriots" or those who don't trust institutions), those who have moral qualms with the organization (e.g., with actions being taken by the military) or misalignment on political issues such as trans rights. Of note, potential moral qualms shift over time; when Trump was in office "Trump Resistors" may have experienced moral qualms, while self-described "patriots" may feel misaligned under Biden.

Work Resentment

A third key motivator for engaging in insider threat is disgruntlement/desire for revenge against one's organization. This could be due to a problematic individual/organization relationship, available through audience segments such as low job satisfaction or disengagement from work. Although Teixeira showed warning signs before and after his entry into the Air National Guard, it was after being disciplined for looking at classified materials that colleagues noted a marked change in his personality. They reported Teixeira seemed like a "completely different person" after being "admonished" and worried that he would "do something drastic" (Lamothe and Harris 2023). Of note, fears at the time were that Teixeira would become an active shooter not a mass leaker; however, this emphasizes the inter-connected nature of various kinds of insider threat perpetration.

In terms of military members specifically, ideological views that lead to a "moral qualm" with the government or military are especially relevant. These could include views on hot button issues such as transgender individuals in the military, the role of the military in certain conflicts, or the very legitimacy of the U.S. government as discussed above.

Conclusion

This paper has demonstrated that commercially available data contains proxy variables which can identify individuals' insider access as well as whether they contain the predispositions and motivations for engaging in actions against their organization. For a small sum of money, external actors can purchase this dataset, allowing them to target thousands of potential insider threats. While not all individuals in the dataset will be potential threats, this data presents a low cost, low risk and potentially high reward endeavor by nefarious actors; only one individual on a list of potentially hundreds or thousands would need to "bite" to be worthwhile. Further, due to the low cost of commercially available data, the kinds of actors able to engage in this effort are broadened. Malicious state actors could purchase the data; however, nonstate actors, and even individuals are able to as well.

Through an analysis of the literature on insider threat and/or a close examination of the available information on previous perpetrators of espionage, mass leaking, and treason, one may curate a list of military members with the common predispositions and recent life stressors that make individuals vulnerable to engaging in insider threat.

Further, once this list is crafted, malign actors could use the available commercial data to understand what would motivate specific individuals to work against their organization and how to best approach them. Essentially, the available commercial data allows for the cultivation of a list potentially containing the next Chelsea Manning or Reality Winner, compiling all individuals possessing the characteristics common to mass leakers who also have classified access.

At the moment of this writing, all of the data collection and selling/sharing practices described above are legal[16] in the U.S. context.[17] This includes when the data is being purchased by individuals who may (or may not) have nefarious intentions, U.S. law enforcement officials,[18] the U.S. intelligence community, or foreign adversaries. Further, with individual records on sale for mere pennies, this data is accessible to nearly anyone with a credit card (Forbrukerrådet 2020, 43). Recently, however, legislators have begun to fight back, pushing for new bills that would limit the ability of data brokers to conduct unfettered trade in Americans' personally identifiable information.[19]

In February of this year, the Biden administration issued an Executive Order calling for the ban of data brokers' ability to sell U.S. bulk sensitive data to "countries of concern,"[20] such as Iran, China, Russia, and North Korea (Biden 2024). These particular transactions are especially concerning due to the potential for blackmail of Americans including U.S. servicemembers and government personnel (McKenna 2024). The EO tasked the Department of Justice with constructing new regulations to prevent the bulk transfer of this data to the aforementioned countries and to empower other federal agencies with stopping the transfer of specific health and genomic data (McKenna 2024; Brown, Chin-Rothmann, and Brock 2024).

These agencies are stepping up in earnest. In March of 2024 the House passed a bill that would ban the sale of sensitive information to foreign adversaries (Feiner

16 While this may seem surprising due to existing laws such as HIPPA, it's important to note that this (and other existing) privacy legislation is entity based. That is, entities like *hospitals* cannot share an individual's health information, however *apps* are under no such legal constraint (Forbrukerrådet 2020, 11).

17 It's worth noting that while this form of data collection and dissemination may be legal in the U.S., in other markets it operates on a shakier foundation. Per a 2020 report by the Consumer Council of Norway, the authors found that much of the data transmission was actually illegal per the General Data Protection Regulation (GDPR) (Forbrukerrådet 2020, 6).

18 In the 2018 landmark court case *Carpenter*, the courts found that law enforcement needed to obtain a warrant in order to access an individual's persistent location data. However, there is a loop hole in the Fourth Amendment protection; when individuals "give consent" to apps to access this data and it is bought and sold through data brokers, law enforcement can then legally purchase the data circumventing the warrant requirement (Brennan, Coulthart, and Nussbaum 2023, 86). The proposed "Fourth Amendment is Not For Sale Act" would explicitly prohibit the sale of this data to the U.S. government and require a court order to obtain GPS data (Chin-Rothmann 2023, 26).

19 At the federal level, multiple bills are being put forth with the aim of curbing data collection and sharing. Many of the propositions would give U.S. citizens the same protections held under the European Union's GDPR which includes the right to view and change information held by brokers (Chin-Rothmann 2023, 25).

20 While discussions of banning particular apps, like TikTok due to its Chinese ownership, dominates the newsfeed, China could just as easily access this information by purchasing it (and much more) from data brokers.

2024) and the Consumer Financial Protection Bureau began debating new regulations that would require data brokers to comply with Fair Credit Reporting Act. In essence, treating them as "consumer reporting agencies" which would ban sharing of certain kinds of data unless there was a "specific purpose outlined in the law" (Del Valle 2024).

Importantly, however, the executive order does not contain information on how brokers must "aggregate, process, store, and share sensitive information" with U.S. entities (Brown, Chin-Rothmann, and Brock 2024) nor does it prohibit the sharing/selling of sensitive information to countries which are not designated as "concerning". This creates an opening for other individuals to buy and resell the information to countries of concern or for these countries to acquire the data through other means such as hacking or intercepting data transmissions. That is, as long as the industry persists, so will the threat.[21]

In the months and years ahead, it will be essential to continue pushing for controls on the collection and dissemination of Americans' personal data. This demands both a legislative and research response. On the legislative end, future bills must work to curtail not only sales to "countries of concern" but the collection and dissemination of this data more broadly. For as long as the industry persists, the data will be at risk of falling into nefarious hands. On the research end, a robust research agenda must be developed and enacted to understand the varying sources of this data, its accuracy, and how/when/by whom this data is being acquired and utilized.

On a final note, it's worth mentioning that due to the nature of this data government entities could purchase it as well in an effort to stem potential insider threats. In fact, in many ways this data is more comprehensive than that which currently underwrites efforts like continuous monitoring. Audience segments include the stressors discussed above as well as comprehensive psychological profiles that tap into individuals' "online lives." However, we argue that U.S. citizens – including service members and their families – would be better served by developing policies to keep this data from being collected, aggregated, and sold indiscriminately. The potential for misuse outweighs positive outcomes.

21 While the EO did set in motion some important legislative changes, McKenna (2024) argues that the order's "larger significance lies in its stated rationale for why the U.S. needs such an order to protect people's sensitive data in the first place." That is, while the EO does not demand a large-scale recalibration of the data broker industry it serves the integral role of informing the public about the "staggering" amount of data that is currently up for sale.

REFERENCES

Allen, Matt, Kat Parsons, Tin Nguyen, and Lauren Zimmerman. 2023. "Examining Best Practices in Threat Assessment from an Insider Threat Perspective." National Counterterrorism Innovation, Technology, and Education Center. https://www.unomaha.edu/ncite/_files/insider-threat-and-threat-assessment-literature-review-website-version96.pdf.

Baker, Peter. 2023. "Robert Hanssen, F.B.I. Agent Exposed as Spy for Moscow, Dies at 79." *The New York Times*, June 5, 2023, sec. U.S. https://www.nytimes.com/2023/06/05/us/robert-hanssen-spy-dead.html.

Bedford, Justine, and Luke Van Der Laan. 2021. "Operationalising a Framework for Organisational Vulnerability to Intentional Insider Threat: The OVIT as a Valid and Reliable Diagnostic Tool." *Journal of Risk Research* 24 (9): 1180–1203. https://doi.org/10.1080/13669877.2020.1806910.

Berry, Christopher M., Deniz S. Ones, and Paul R. Sackett. 2007. "Interpersonal Deviance, Organizational Deviance, and Their Common Correlates: A Review and Meta-Analysis." *Journal of Applied Psychology* 92 (2): 410–24. https://doi.org/10.1037/0021-9010.92.2.410.

Biddle, Sam, and Jack Poulson. 2022. "American Phone-Tracking Firm Demo'd Surveillance Powers by Spying on CIA and NSA." The Intercept. April 22, 2022. https://theintercept.com/2022/04/22/anomaly-six-phone-tracking-zignal-surveillance-cia-nsa/.

Biden, Joseph R. 2024. "Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." The White House. February 28, 2024. https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.

Bowling, Nathan A., Gary N. Burns, Susan M. Stewart, and Melissa L. Gruys. 2011. "Conscientiousness and Agreeableness as Moderators of the Relationship Between Neuroticism and Counterproductive Work Behaviors: A Constructive Replication: Personality and CWBS." *International Journal of Selection and Assessment* 19 (3): 320–30. https://doi.org/10.1111/j.1468-2389.2011.00561.x.

Brennan, Shelby, Stephen Coulthart, and Brian Nussbaum. 2023. "The Brave New World of Third Party Location Data." *Journal of Strategic Security* 16 (2): 81–95. https://doi.org/10.5038/1944-0472.16.2.2070.

Brown, Evan, Caitlin Chin-Rothmann, and Julia Brock. 2024. "Exploring the White House's Executive Order to Limit Data Transfers to Foreign Adversaries," February. https://www.csis.org/analysis/exploring-white-houses-executive-order-limit-data-transfers-foreign-adversaries.

Burgess, Matt. 2022. "Their Photos Were Posted Online. Then They Were Bombed." *Wired UK*, August 26, 2022. https://www.wired.co.uk/article/wagner-group-osint-russia-ukraine.

Chin-Rothmann, Caitlin. 2023. "Surveillance for Sale," CSIS Strategic Technologies Program, , June, 1–55.

Cybersecurity and Infrastructure Security Agency (CISA). 2020. "ISC Violence in the Federal Workplace Guide | CISA." December 17, 2020. https://www.cisa.gov/resources-tools/resources/isc-violence-federal-workplace-guide.

Del Valle, Gaby. 2024. "The CFPB Wants to Rein in Data Brokers - The Verge." The Verge. April 15, 2024. https://www.theverge.com/2024/4/15/24131354/cfpb-data-brokers-fair-credit-reporting-act.

Department of Homeland Security. 2019. "Department of Homeland Security Strategic Framework for Countering Terrorism and Targeted Violence." https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorismtargeted- violence.pdf.

Donnan, Shawn, and Dina Bass. 2022. "How Did ID.Me Get Between You and Your Identity?" *Bloomberg.Com*, January 20, 2022. https://www.bloomberg.com/news/features/2022-01-20/cybersecurity-company-id-me-is-becoming-government-s-digital-gatekeeper.

Ellen, B. Parker, Katherine C. Alexander, Jeremy D. Mackey, Charn P. McAllister, and Jack E. Carson. 2021. "Portrait of a Workplace Deviant: A Clearer Picture of the Big Five and Dark Triad as Predictors of Workplace Deviance." *Journal of Applied Psychology* 106 (12): 1950–61. https://doi.org/10.1037/apl0000880.

Feiner, Lauren. 2024. "House Passes Bill to Prevent the Sale of Personal Data to Foreign Adversaries." The Verge. March 20, 2024. https://www.theverge.com/2024/3/20/24106991/house-data-broker-foreign-adversaries-bill-passes.

Forbrukerrådet. 2020. "OUT OF CONTROL: How Consumers Are Exploited by the Online Advertising Industry." The Consumer Council of Norway. https://www.forbrukerradet.no/out-of-control/.

Galić, Zvonimir, and Mitja Ružojčić. 2017. "Interaction between Implicit Aggression and Dispositional Self-Control in Explaining Counterproductive Work Behaviors." *Personality and Individual Differences* 104 (January): 111–17. https://doi.org/10.1016/j.paid.2016.07.046.

Greitzer, Frank L., and Ryan E. Hohimer. 2011. "Modeling Human Behavior to Anticipate Insider Attacks." *Journal of Strategic Security* 4 (2): 25–48. https://doi.org/10.5038/1944-0472.4.2.2.

Harris, Shane, and Samuel Oakford. 2023. "Jack Teixeira Got Security Clearance despite History of Violent Threats." Washington Post. December 11, 2023. https://www.washingtonpost.com/national-security/2023/12/11/jack-teixeira-discord-leaks/.

Herbig, Katherine L. 2017. "The Expanding Spectrum of Espionage by Americans, 1947-2015." https://apps.dtic.mil/sti/citations/AD1040851.

Hsu, Jeremy. 2018. "The Strava Heat Map Shows Even Militaries Can't Keep Secrets from Social Data." *Wired*, January 29, 2018. https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

Hugl, Ulrike. 2010. "The Malicious Insider Problem: An Integrated View on Individual, Organizational and Contextual Influencing Factors." In , 93–101. Thessaloniki, Greece.

REFERENCES

Ikeda, Scott. 2020. "Many of the Major Dating Apps Are Leaking Personal Data to Advertisers." CPO Magazine (blog). January 30, 2020. https://www.cpomagazine.com/data-privacy/many-of-the-major-dating-apps-are-leaking-personal-data-to-advertisers/.

Irvin, John a, and David L. Charney. 2014. "Stopping the Next Snowden." *POLITICO Magazine*. March 25, 2014. https://www.politico.com/magazine/story/2014/03/stopping-next-edward-snowden-105004.

Johnson, Khari. 2023. "Algorithms Allegedly Penalized Black Renters. The US Government Is Watching." *Wired*, January 16, 2023. https://www.wired.com/story/algorithms-allegedly-penalized-black-renters-the-us-government-is-watching/.

Keegan, Jon, and Joel Eastwood. 2023. "From 'Heavy Purchasers' of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You – The Markup." June 8, 2023. https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you.

Koch, Richie. 2024. "How to Protect Your Privacy on Dating Apps | ProtonVPN." Proton VPN Blog. February 12, 2024.

Kranefeld, Iris, and Gerhard Blickle. 2022. "Disentangling the Relation between Psychopathy and Emotion Recognition Ability: A Key to Reduced Workplace Aggression?" *Personality and Individual Differences* 184 (January): 111232. https://doi.org/10.1016/j.paid.2021.111232.

Lamothe, Dan, and Shane Harris. 2023. "Accused Leaker Teixeira Was Seen as Potential Mass Shooter, Probe Finds." *Washington Post*, December 23, 2023. https://www.washingtonpost.com/national-security/2023/12/22/teixeira-investigation-active-shooter-threat/.

Lenzenweger, Mark F., and Eric D. Shaw. 2022. "The Critical Pathway to Insider Risk Model: Brief Overview and Future Directions." *Counter-Insider Threat Research and Practice* 1 (1).

Liao, Zhenyu, Hun Whee Lee, Russell E. Johnson, Zhaoli Song, and Ying Liu. 2021. "Seeing from a Short-Term Perspective: When and Why Daily Abusive Supervisor Behavior Yields Functional and Dysfunctional Consequences." *Journal of Applied Psychology* 106 (3): 377–98. https://doi.org/10.1037/apl0000508.

Liptak, Andrew. 2018. "Hackers Accessed More Personal Data from Equifax than Previously Disclosed - The Verge." The Verge. February 11, 2018. https://www.theverge.com/2018/2/11/17001046/equifax-hack-personal-data-tax-identification-numbers-email-addresses-drivers-licenses-cybersecurity.

Mackey, Jeremy D., Rachel E. Frieder, Jeremy R. Brees, and Mark J. Martinko. 2017. "Abusive Supervision: A Meta-Analysis and Empirical Review." *Journal of Management* 43 (6): 1940–65. https://doi.org/10.1177/0149206315573997.

Marks, Joseph. 2014. "Aiming to Stop the next Snowden." POLITICO. September 17, 2014. https://www.politico.com/story/2014/09/pentagon-edward-snowden-111030.

McKenna, Anne Toomey. 2024. "Biden Executive Order on Sensitive Personal Information Does Little for Now to Curb Data Market – but Spotlights the Threat the Market Poses." The Conversation. March 2, 2024. http://theconversation.com/biden-executive-order-on-sensitive-personal-information-does-little-for-now-to-curb-data-market-but-spotlights-the-threat-the-market-poses-224702.

Nechepurenko, Ivan. 2019. "Russia Votes to Ban Smartphone Use by Military, Trying to Hide Digital Traces." *The New York Times*, February 19, 2019, sec. World. https://www.nytimes.com/2019/02/19/world/europe/russia-military-social-media-ban.html.

O'Boyle, Ernest H., Donelson R. Forsyth, George C. Banks, and Michael A. McDaniel. 2012. "A Meta-Analysis of the Dark Triad and Work Behavior: A Social Exchange Perspective." *Journal of Applied Psychology* 97 (3): 557–79. https://doi.org/10.1037/a0025679.

Occupational Safety and Health Administration (OSHA). 2016. "Guidelines for Preventing Workplace Violence for Healthcare and Social Service Workers (OSHA 3148-06R 2016)." U.S. Department of Labor: OSHA. https://www.osha.gov/sites/default/files/publications/OSHA3148.pdf.

Philip Legg, Nick Moffat, Jason R.C. Nurse, Jassim Happa, Ioannis Agrafiotis, Michael Goldsmith, and Sadie Creese. 2013. "Towards a Conceptual Model and Reasoning Structure for Insider Threat Detection." *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 4 (4): 20–37. https://doi.org/10.22667/JOWUA.2013.12.31.020.

Postma, Foeke. 2021. "US Soldiers Expose Nuclear Weapons Secrets Via Flashcard Apps." Bellingcat. May 28, 2021. https://www.bellingcat.com/news/2021/05/28/us-soldiers-expose-nuclear-weapons-secrets-via-flashcard-apps/.

Rizvi, Hur-Ali, and Melinda Fern. 2021. "Data Privacy and Dating Apps: Dangerous Implications for the LGBTQ+ Community." *Foundation for a Human Internet* (blog). June 30, 2021. https://medium.com/humanid/data-privacy-and-dating-apps-dangerous-implications-for-the-lgbtq-community-345b70643491.

Runge, J. Malte, Jonas W.B. Lang, Ingo Zettler, and Filip Lievens. 2020. "Predicting Counterproductive Work Behavior: Do Implicit Motives Have Incremental Validity beyond Explicit Traits?" *Journal of Research in Personality* 89 (December): 104019. https://doi.org/10.1016/j.jrp.2020.104019.

Shaw, Eric, and Laura Sellers. 2015. "Application of the Critical-Path Method to Evaluate Insider Risks." I*nternal Security and Counterintelligence* 59 (2): 1–8.

Sherman, Justin. 2021. "Data Brokers Are Advertising Data on U.S. Military Personnel." Lawfare. August 23, 2021. https://www.lawfaremedia.org/article/data-brokers-are-advertising-data-us-military-personnel.

Sherman, Justin, Hayley Barton, Aden Klein, Brady Kruse, and Anushka Srinivasan. 2023. "Data Brokers and the Sale of Data on U.S. Military Personnel." Duke University. https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/.

Simmons, Alistair, and Justin Sherman. 2022. "Data Brokers, Elder Fraud, and Justice Department Investigations." Lawfare. July 25, 2022. https://www.lawfaremedia.org/article/data-brokers-elder-fraud-and-justice-department-investigations.

REFERENCES

Stack, Megan K. 2022. "Opinion | She Tried to Resist and Found Herself Alone." *The New York Times*, December 6, 2022, sec. Opinion. https://www.nytimes.com/2022/12/06/opinion/reality-winner.html.

Szalavitz, Maia. 2021. "The Pain Was Unbearable. So Why Did Doctors Turn Her Away?" *Wired*, August 11, 2021. https://www.wired.com/story/opioid-drug-addiction-algorithm-chronic-pain/.

Thompson, Stuart A., and Charlie Warzel. 2019. "Opinion | Twelve Million Phones, One Dataset, Zero Privacy." *The New York Times*, December 19, 2019, sec. Opinion. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

Thompson, Terence J. 2014. "Toward an Updated Understanding of Espionage Motivation." *International Journal of Intelligence and CounterIntelligence* 27 (1): 58–72. https://doi.org/10.1080/08850607.2014.842805.

——. 2018. "A Psycho-Social Motivational Theory of Mass Leaking." *International Journal of Intelligence and CounterIntelligence* 31 (1): 116–25. https://doi.org/10.1080/08850607.2017.1374800.

Viñas-Racionero, Rosa, Mario J. Scalora, and James S. Cawood. 2021. "Workplace Violence Risk Instrumentation: Use of the WAVR-21 V3 and the CAG." In *International Handbook of Threat Assessment*, by Rosa Viñas-Racionero, Mario J. Scalora, and James S. Cawood, edited by J. Reid Meloy and Jens Hoffmann, 522–35. Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0030.

Warren, Tom. 2018. "Marriott Reveals Massive Database Breach Affecting up to 500 Million Hotel Guests." The Verge. November 30, 2018. https://www.theverge.com/2018/11/30/18119403/marriott-database-breach-starwood-hotels.

White, Stephen G. 2021. "Workplace Targeted Violence: Assessment and Management in Dynamic Contexts." In *International Handbook of Threat Assessment*, by Stephen G. White, edited by J. Reid Meloy and Jens Hoffmann, 107–35. Oxford University Press. https://doi.org/10.1093/med-psych/9780190940164.003.0006.

Whitty, Monica T. 2021. "Developing a Conceptual Model for Insider Threat." *Journal of Management & Organization* 27 (5): 911–29. https://doi.org/10.1017/jmo.2018.57.

Wilder, Ursula M. 2017. "The Psychology of Espionage." *Studies in Intelligence* 61 (2): 19–36.

Zhao, Lijing, Long W. Lam, Julie N. Y. Zhu, and Shuming Zhao. 2022. "Doing It Purposely? Mediation of Moral Disengagement in the Relationship Between Illegitimate Tasks and Counterproductive Work Behavior." *Journal of Business Ethics* 179 (3): 733–47. https://doi.org/10.1007/s10551-021-04848-7.

Zhou, Zhiqing E., Laurenz L. Meier, and Paul E. Spector. 2014. "The Role of Personality and Job Stressors in Predicting Counterproductive Work Behavior: A Three-way Interaction." *International Journal of Selection and Assessment* 22 (3): 286–96. https://doi.org/10.1111/ijsa.12077.

Table 3. Insider Threat Framework with (selected) Proxy Variables from Commercial Data

Category	Sub-Category	Exemplar Variables	Exemplar Variables
Predispositions	Personality	Dark Triad	• Eyeota – FI NDR – Insight360 – Values360 – 2 Self-centered and passive • VisualDNA Mobile & App > Personality > UK > Agreeableness > Self Focused
		Big 5	• VisualDNA Personality – US – Agreeableness – Lone Wolves • VisualDNA Personality – US – Neuroticism – Trapped • VisualDNA Personality – US – Conscientiousness – Spontaneous Coasters
		Other Traits of Interest	• Eyeota – US Experian – Psychographic / Attitudes – Self Concept – Dominating / Authoritarian • VisualDNA Personality – Personality – Agreeableness – Control Seekers • VisualDNA Personality – US – Neuroticism – Stress Reactors • Eyeota – US Experian – Psychographic / Attitudes – Personal Views – Social Isolation • Eyeota – AU RDA Research – Consumer Profiles – Demo – General Attitudes – I generally get a raw deal out of life • Branded Data > Connexity > CNX Lifestyle > The Adrenaline Junkie (BlueKai)
	Psychosocial Traits	Substance Abuse	• Skydeo > ConditionGraph > Health & Wellness > Lifestyle Indicators > Alcohol: Drink & Drive
		Mental Health	• Kantar > US > Custom > Use Any Rx Treatment for Depression • Eyeota – US Kantar – Health and Wellness – Conditions and Treatments – Post Traumatic Stress Disorder or Ptsd
	Demographics	Gun Ownership	• Neustar AdAdvisor > AdAdvisor Political Audiences > Outlook > Gun Owners
Stressors	Family	Marriage/Divorce	• Branded Data > Media Source > Demographic > Family Composition > Marital Status > Recent Divorce (BlueKai) • Branded Data > Experian > Life Event > Recently Married > Last 3 Months (BlueKai)
		Pregnancy	• Predictive Audience > Eyeota > Demo > US – Life Events – Expectant Mothers / Pregnancy
		Terminal Illness	• Consumer > Healthcare > Healthcare – Terminal Illness & Counseling
		Recent Death	• Adyoulikesa_bereavement
		Frequent Moving	• Eyeota – DE Schober – Living Environment – Moving Frequency – High Fluctuation
	Work	Low Job Satisfaction	• Skydeo > ConditionGraph > Health & Wellness > Job Satisfaction > Low Job Satisfaction
		Moral Qualm with organization	
Motivations	Financial	Loans	• Branded Data > Gravy Analytics > In-Market > In-Market Payday Loans (BlueKai)
		Debt	• Zipline Estimated Household Debt Level $75,000 +
		Bankruptcy	• Companies In-Market for Goods & Services > Financial Services – Bankruptcy & Insolvency (Adstra)
		Financial Changes	• Powerlytics Stirista Fusion > Income Changes > Disposable Income 5 Year Percent Change > Disposable Income Decrease 75+% in the Last 5 Years
		Gambling	• Clickagy > Health > Addictions > Gambling

Table 3. Insider Threat Framework with (selected) Proxy Variables from Commercial Data *(Cont'n)*

Category	Sub-Category	Exemplar Variables	Exemplar Variables
Motivations	Ideological	Immigration	• Infogroup > B2C > Politics > Issues > Immigration > Mexican Border Wall > Supporters – Co-op Sourced
		LGBTQ+	• Social Profiles by Type > Lesbian/Gay/Bisexual/Transgender (LGBT) Supporters (Adstra) • Infogroup > B2C > Politics > Issues > Social > Transgender Bathroom Rights > Opponents – Co-op Sourced
		Abortion	• Infogroup > B2C > Politics > Issues > Social > Abortion Rights > Pro Life Supporter – Co-op Sourced • Infogroup > B2C > Politics > Issues > Social > Abortion Rights > Pro Choice Supporter – Co-op Sourced
		Guns	• Social Profiles by Type > 2nd Amendment Supporters (Adstra) • Social Profiles by Type > Gun Control Supporters (Adstra) • Infogroup > Consumer > US Politics > Issues & Advocacy > Registered Gun Owner Concealed Permit
		Conspiracy	• Audiences by Oracle > Consumer Packaged Goods (CPG) > Datalogix (DLX) Purchase-Based > BuyStyles > Non-GMO (BlueKai) • Consumer > Media > Right Wing Blogs – Conspiracy Theories (Dstillery) • Branded Data > Gravy Analytics > Lifestyle > Survivalist Prepper Interest (BlueKai)
		Trust in Institutions (media, banks, govt, social media)	• Neustar AdAdvisor > Attitudes > > Uncomfortable trusting money to a Bank • Fluent > TS Modeled > COVID 2021 > Not Planning to Get Vaccine > Dont Trust Vaccines • Infogroup > Consumer > US Politics > Media Consumption > News Source–Most Trusted Source – FOX • Infogroup > Consumer > US Politics > Media Consumption > News Source–Most Trusted Source – MSNBC • Nielsen Movies – Entertainment Behaviors – Trust Social Media Posts from Friends/Family (NRG) (Exelate) • Eyeota – FI NDR – Insight360 – Values360 – 4 Patriots seeking security • L2 Voter Data > Individual Demographics > Parties Description > Patriot
		Political Alignment	• Branded Data > ALC > Aristotle Political Precision (US) > Political Affiliation by Party > Conservative-Very Conservative (BlueKai) • Affluent Consumers by Political Affiliation > Democrat (Adstra) • Political Affiliations :: Trump Resistor :: (All) • Political Affiliations :: Trump Supporter :: (All)
	Disgruntlement/ Revenge Against Organization	Disengaged Worker	• VisualDNA > Personality > UK > Resourcefulness > Disengaged Workers
		Overqualified Worker	• VisualDNA > Personality > US > Resourcefulness > Overqualified Workers
		Low Job Satisfaction	• Skydeo > ConditionGraph > Health & Wellness > Job Satisfaction > Low Job Satisfaction
		Ideological Misalignment with Organization (e.g. moral qualm)	• See ideology section and political alignment

The Use of Military Narratives in White Supremacist Chatrooms on Telegram

Dana B. Weinberg
Noah D. Cohen
Meyer Levy
Yunis Ni

Abstract

This study investigates the connections between military and white supremacist narratives in extremist channels on the social media platform Telegram. It explores military narratives as both a source of and impetus to insider threat. Narratives about the military, when combined with extremist narratives, can redirect antipathies toward legitimate leadership and drive individuals to commit violence or betray institutions. Moreover, the co-opting of military narratives to support extremism may serve to undermine public trust in and support for the military itself, posing an additional threat to national security.

Scraping data from 224 public Telegram channels between September 2016 and October 2020 and selecting posts that contain military terminology, we explore connections between white supremacist and military narratives through the use of supervised machine learning techniques. We hand-code small portions of our corpus (training set) for these narratives and then label the remaining data (test set) using a machine learning classification process. The results enable analysis of the narrative network underlying the corpus.

We find that white supremacist narratives are prevalent in posts with military-terminology and frequently appear alongside military narratives. The corpus is dominated by what previous research has termed "extinction narratives," or narratives which predict the destruction of one's cultural group. Such narratives are capable motivators of violence. Military actors and themes often form the backdrop for these narratives, which vilify Jews as evil infiltrators of American institutions and cast whites as innocent victims of their machinations and of government betrayal. Military narratives lend urgency and legitimacy to these narratives that underscore white superiority and threats to the white race.

DANA B. WEINBERG

Dana Beth Weinberg, Director of the New War Research Consortium, is Professor of Sociology and Data Science at Queens College and The Graduate Center-City University of New York. Dr. Weinberg holds a PhD from Harvard University. At Queens College, she has served as Acting Dean of Social Sciences, Chair of Sociology, and Director of the MA Program in Data Analytics and Applied Social Research. She is the author of *Code Green: Money-Driven Hospitals and the Dismantling of Nursing*. Her current work focuses on foreign and domestic influence operations on social media, narrative weaponization and hate speech, insider threat, and the social factors that enable individual and organizational resilience.

NOAH D. COHEN

Noah D. Cohen is a Criminal Justice Ph.D. student at John Jay College of Criminal Justice and the CUNY Graduate Center in New York City. He received his M.S. in Criminal Justice and Criminology from San Diego State University and his B.A. from the University of California – Santa Barbara. His research is focused primarily on antisemitism and hate crime trends and analysis, as well as political radicalization, and investigation into environmental and wildlife crimes.

The particular combination of military and white supremacist narratives is a cause for alarm. Military personnel are high-value recruitment targets for extremist organizations due to their competence and appearance of legitimacy. The narrative network we describe provides insight into how military valor may be stolen and usurped for extremist causes and how military targets may be lured to political violence in service to them.

Introduction

Understanding the Military as a Target for Extremist Radicalization

The participation of military members in the events on January 6th, 2021, reinvigorated concerns regarding the presence of political extremism within the U.S. military (Mitchell 2021; Stafford and LaPorta 2021) and the related potential for insider threat. In a study of 716 individuals arrested for their participation in January 6th, Denbeaux and Crawley (2023) found that 105, almost 15%, had a military background. Of these, 31 were members of the Proud Boys, Oath Keepers, or Three Percenters (Denbeaux and Crawley 2023), which are all extremist groups. These relatively high levels of military participation have raised concerns that the military has an extremism problem. Extremist groups have long been suspected of targeting current and former military members for recruitment, if not joining the military themselves, due to the perceived benefits of military experience on extremists' lethality and operational effectiveness (Chermak, Freilich, and Suttmoeller 2013; Simi, Bubolz, and Hardman 2013; B. L. Smith et al. 2011). Successfully radicalized military personnel

MEYER LEVY

Dr. Meyer Levy is a research associate with the New War Research Consortium. Prior to this appointment, he was a visiting scientist at the National Geospatial-Intelligence Agency. He received his Ph.D. in political science from the University of Notre Dame, and wrote his dissertation on political speech on Reddit and 4chan.

YUNIS NI

Yunis Ni received a B.S. in Design from the Fashion Institute of Technology. She is finalizing her M.A. in Data Analytics at Queens College and is a graduate associate and researcher with the New War Research Consortium.

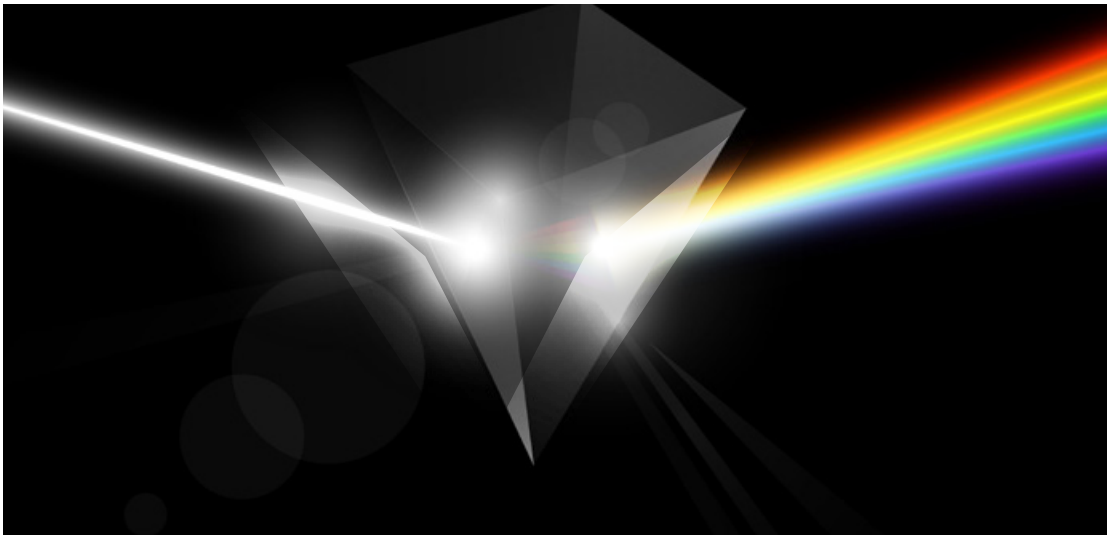
embody potentially destructive insider threats to the U.S. military (Lang 2022; Ware 2023). In this case, insider threat refers to servicemembers or veterans using their special insider knowledge and/or access to betray the government, the nation, or the military.

There have been several examples of this type of insider threat related to extremist, specifically to white supremacist, ideology. Former U.S. Army Private Ethan Melzer conspired with members of the Neo-Nazi organization, the Order of the Nine Angles, to attack members of his unit (U.S. Department of Justice Office for Public Affairs 2020; Ware 2023), sending "sensitive details about his unit – including information about its location, movements, and security..."(U.S. Department of Justice Office for Public Affairs 2020). In another case, Former Airman First Class Andrew Dornan was dishonorably discharged in June 2006, and was reported to have declared support for Adolf Hitler and threatened to bomb a military base (Holthouse 2006; Ware 2023). Former Coast Guard Lieutenant Christopher Hasson was arrested on February 15, 2019, having written a manifesto expressing desires to enact violence to "establish a white homeland" and towards suspected "traitors" (McCausland 2019), which included Democratic members of Congress and several Supreme Court Justices (McCausland 2019; Myre and Romo 2019). More recently, Former Air Force National Guardsman Jack Teixeira was arrested on April 13, 2023, for leaking a number of classified intelligence documents to servers on Discord (Harris, Oakford, and Dehganpoor 2023; U.S. Department of Justice Office for Public Affairs 2023). While Teixeira appeared to be motivated primarily by a desire for fame amongst his followers on Discord (Harris, Oakford, and Dehganpoor 2023; Rawnsley and LaPorta 2023), he also subscribed

> **This use of military symbolism by violent extremists may undermine civilian trust in and support for military institutions, with potential consequences for military recruitment, preparedness, and strength**

to anti-government and white supremacist ideologies (Hoffman and Ware 2024). Together, these cases exemplify the potential for insider threat from military personnel with ties to extremist groups and ideologies.

In addition to radicalization of current and former servicemembers, another source of insider threat is the use of militaristic language, symbols, paraphernalia, and/or pretense of having served by extremists. In essence, this use amounts to stolen valor, claiming unearned military status and heroism. Such co-option of military symbols and imagery may help them conceal the true nature of their extremism (Schake and Robinson 2021) under the guise of military discipline and patriotism (Schrama 2023), as well as brand themselves as true and authentic defenders of the nation (e.g., Freilich, Pienik, and Howard 2001; Schrama 2023). This use of military symbolism by violent extremists may undermine civilian trust in and support for military institutions, with potential consequences for military recruitment, preparedness, and strength (Schake and Robinson 2021; Ware 2023; Schrama 2023).



> **...intentional pairing of mainstream and extremist narratives may a point of departure for mainstream audiences to accept fringe narratives**

In this paper, we combine social science and computer science approaches to consider the role of military narratives in white supremacist discourse. We define narratives (as detailed in the Methods section) as stories about events and their characters or actants. We examine the most common narratives in white supremacist conversations containing military-related terminology and the network of prominent narratives within these conversations. The use of military stories and protagonists may serve both to aid recruitment of current and former servicemembers as well as develop an association between these widely recognized narratives and protagonists and calls for political violence (Weinberg and Dawson 2021). Our findings have implications for studies of insider threat, recruitment into extremist organizations, the development of conspiracy theories, and other related fields.

Theoretical Framework and Hypotheses

Narratives draw their power from the connections they make to other stories of cultural relevance or significance (Polletta 2008; Polletta and Callahan 2017). When connected to other narratives of ingroup threat, they can engender fears of cultural extinction, and drive their audiences to follow through on violent calls to action (Marcks and Pawelz 2022).

The content network surrounding narratives is of particular importance to understanding how and why they are deployed. Media which contains multiple narratives are able to invoke deeper meanings or provide greater emotional resonance (Polletta and Callahan 2017; Weinberg and Dawson 2021; Dawson and Weinberg 2020; Weinberg, Dawson, and Edwards 2022). Narrative combination can also smooth the delivery of a complex moral message. For example, when military narratives of soldiers' sacrifice are combined with narratives of government betrayal, one can deliver a message which is at once anti-government and patriotic (Dawson and Weinberg 2020). Moreover, intentional pairing of mainstream and extremist narratives may provide a point of departure for mainstream audiences to accept fringe narratives (Weinberg and Dawson 2021). Far-right extremists, as discussed above, are frequently attracted to military rhetoric for its legitimizing potential. Military rhetoric enables extremists to portray themselves as sincere patriots and competent political actors (Furlow and Goodall 2011; Marcks and Pawelz 2022; Freilich, Pienik,

> **Moreover, intentional pairing of mainstream and extremist narratives may a point of departure for mainstream audiences to accept fringe narratives.**

and Howard 2001; Schake and Robinson 2021), and we suggest that one way they do this is through sharing military narratives. Combining military narratives with extremist narratives may furthermore offer audiences a familiar and patriotic narrative that serve to legitimize and make palatable the accompanying extremist narratives.

Military narratives may also lend emotional urgency to extremist messaging. Studies have long found that the use of militaristic language and symbols in political messaging heightens the perceived severity of the threats facing a particular social group (Flusberg, Matlock, and Thibodeau 2018; Furlow and Goodall 2011; Schnepf and Christmann 2022). Militaristic rhetoric imbues narratives with a war-like framing, which elevates conflict to an inherently gruesome struggle for survival against an outgroup. Marcks and Pawelz (2022) define such stories which predict the demise of one's ingroup as an "extinction narrative." P. Smith (2005) finds that such narratives typically call for collective mobilization against an absolute evil which, beyond threatening merely a single group, threatens the "planet or civilization" as a whole (P. Smith 2005, p. 26-27).

In short, we anticipate that military narratives will play a key role in the narrative content network in white supremacist chatroom messages on Telegram that contain military language. We expect that they will serve as a key connector and driver of meaning within the network and that they will lend greater urgency and legitimacy to white supremacist narratives. Given that our data are selected on the presence of military keywords, we hypothesize that narratives drawn from these data will involve the military or soldiers as key actants—whether protagonists, antagonists, or villains—more frequently than other actants (H1). Furthermore, given that Telegram is a hub for extremist communities (Schulze et al. 2022; Urman and Katz 2022), we expect their conversations will connect military and extremist narratives. We hypothesize that military narratives will have high degree centrality in this content network, making them a key connector between various narrative pathways (H2). Specifically, we hypothesize that military-focused narratives are embedded in a content network of white supremacist narratives, including antisemitic, anti-government, and race theory narratives (H3). Finally, we hypothesize that military narratives will lend urgency to this broader set of white supremacist narratives (H4).

Methods

Data

The data were collected from September 2016 to October 2020 by the Institute for Strategic Dialogue (Davey and Weinberg 2021). They are drawn from 224 far-right channels on Telegram, which were selected based on the use of white supremacist rhetoric. From these channels, 1,091,878 messages were retrieved, and then filtered using a set of 266 keywords related to the military. The final dataset consisted of 14,000 messages. Using the methods outlined below, we code for 30 narratives in 3,750 sentences and then use them to train a classifier to detect them across all 14,000 messages.

Narrative Detection and Identification

We use both Social Science and Computer Science approaches to detect and identify narratives, combining a researcher-driven, content expert approach with computer-driven approaches. Sociologists Poletta and Calahan note that the most powerful narratives may often be invoked through mere reference to their protagonists (or central actors), for example, David and Goliath (Polletta and Callahan 2017). Following this insight, our narrative detection methods focus on identification of the protagonist, antagonist, and other characters or events central to a given story. We, therefore, use a character-based model (Shahsavari et al. 2020; Tangherlini et al. 2020) or what is also called an "entity-based model" (Chambers and Jurafsky 2009) derived from Computer Science. Following the touchstone work of Chambers and Jurafsky (2009), we operationalize our entity-based narrative references as a "a tuple of an event (most simply a verb) and its participants, represented as typed dependencies … of the protagonist: (event, dependency)." (p. 791).

Following a process described in Tangherlini et al. (2020), we break the posts down by sentence and then use a Named Entity Recognition model, which maps words to their part-of-speech tags to identify actants (Ranade et al. 2022). We identify entities using Flair, a Python package. We also replace pronouns with their absolute referent using co-reference resolution. We then go sentence by sentence to identify relationships (arg1, rel, arg2). The package then extracts entities from these relationships, and we count them, as do Shahsavari et al. (2020). Thus, the entity count represents how often the entity appears in relationships in the corpus.

From this first-round identification, similar actants may be combined together. For example, "man," "men," "guys," and "fathers" are combined into a category representing "men." Shasavari et al. (2020) terms these aggregate categories "supernodes" and their individual components "subnodes." Using the top 20 entities, excluding countries, we have five entities that appear most frequently: Jews, government,

military, men, and Whites. We code the 400 most frequent entities for inclusion in these five actant supernodes.

Our researcher-driven approach to identifying narratives uses a combination of predetermined labels as well as labels derived while coding our data. We create a practice coding sheet of narratives for each of the five actant supernodes. Multiple coders refine decision criteria for narrative identification and add or modify narratives to the set for coding as needed. Once the narrative list and the decision criteria are finalized for each actant, we create a randomly selected dataset of about 900 sentences for each entity, a total of 4,507 sentences in all, and code each sentence for the presence of their respective entity-specific narratives. Multiple coders independently code the same textual data. Inter-rater reliability between coders is high across each narrative set, with average agreement scores between 0.88 and 0.94. A selection is coded as containing the narrative when the majority of coders agree. Table 1 shows all of the military-focused narratives codes used in our training data.

Most of the narrative codes focus on a core narrative. For example, the code "warriors are virtuous" relates to a host of narratives about specific warriors or soldiers and their heroic deeds or attributes. The one exception to this core narrative approach is a catch-all narrative code labeled "miscellaneous military narratives." This code identifies posts which contain actions by military actors. Rather than represent a single narrative as our other codes do, the code applies to a wide variety of military narratives reflecting a range of time periods, groups, and geographies. Some of them recount the history of ancient empires such as Rome and Persia while others detail contemporary military activity.

Using the narrative codes that appeared at least ten times on any given actant list as targets, we generate BERT (Bidirectional Encoder Representations from Transformers, a machine learning large language model) embeddings for each sentence (Devlin et al. 2019). We train individual narrative classifiers that estimate the probability, expressed as a binary outcome (present or not present), of the presence of a single narrative within a sentence and then resample to improve classifier performance. We also train ensemble classifiers that predict the full set of narratives within a sentence for each actant. Our classifiers are fit in Python, using the scikit-learn library (Pedregosa et al. 2011). The individual classifiers are instances of scikit-learn's SVM class, and the ensemble classifiers are instances of the MLPClassifier class. BERT embeddings are generated using the 'bert-base-uncased' model, provided by HuggingFace.io through the Transformers library (Wolf et al. 2020). When resampling cases for our individual narrative classifiers, we use the SMOTE class from the imblearn library (Lemaître, Nogueira, and Aridas 2017).

Table 1. Frequency of Military Narratives in Hand-Coded Data

Miscellaenous Military Narratives	119
Warriors Are Virtuous	60
Military Sacrifice Their Lives	54
Military Betrays Society	36
Society Betrays Military	24
Military Betrays Government	21
Military Is a Jewish Puppet	18
Military Defends Nation	18
Government Betrays Military	18
Military Fights Race War	9
Military Is Israel's Puppet	6
Military Is Slave to Government	6
Woke Military Is Weak	6
Military Is Racist Organization	6
Military Betrays Warriors	6
Soldiers Are Suckers and Losers	0

Our individual narrative classifiers are Support Vector Machines, simple yet robust models that have been widely used in the field of text analysis (Cortes and Vapnik 1995). Our ensemble classifiers are Multi-Layer Perceptrons— essentially simple neural networks consisting of just a few hundred neurons and capable of having a wide variety of outputs, including our multi-outcome narrative annotations (Rumelhart, Hinton, and Williams 1986).

Table 2 shows the F1 scores for classification accuracy of each individual narrative using the final output from our ensemble models. Overall, these scores are relatively high, with an average of 0.894, and suggest that our predictions are accurate enough for use in our analysis. The full row agreement in Table 2 represents the percentage of the time that the ensemble classifiers perfectly predict all narrative outcomes for a sentence within a particular actant group, again showing sufficiently high performance scores, with an average of 0.91. Confusion matrices (not shown) indicate that our ensemble classifiers have a balanced number of Type 1 and Type 2 errors and represent a non-trivial solution.

Table 2. Classification Accuracy Scores by Entity Group

Narrative Set	Lowest	Highest	F1 Average	Full Row Agreement
Government	0.801	0.980	0.870	0.951
Jews	0.740	0.978	0.821	0.873
Men	0.900	1.00	0.925	0.991
Military	0.878	1.00	0.965	0.879
White Race	0.735	0.883	0.946	0.874

We use our classifier models to code all sentences in the dataset. For each actant subnode contained within a sentence, we apply the actant's individual narrative classifier, and multiple classifiers are applied when sentences contain more than one of our five actant supernodes. The outputs from these classifiers are then concatenated, producing a set of probabilities for the proximity of the sentence to each narrative. These probabilities are input to the ensemble classifier, which outputs a complete set of codes with binary outcomes for each narrative. The outputs from these various classifiers are concatenated after this process, along with values of '0' to represent narratives for which an appropriate entity was not present.

Analysis

We examine the frequency of the military as a key actant relative to the other top entities in the sentences extracted from the full dataset. Next, we examine the frequency of military narratives, both those featuring the military as main actant and those that also feature other actants, relative to the others in our set. For example, the narrative "government betrays the military" would appear as a government narrative, but it is also a military narrative. We then examine the frequency of narratives by actant.

We next examine the narrative content network, examining how often narratives co-occur in the same post. We calculate the degree centrality of the various military narratives in this network and the narratives to which they have the strongest connections (highest edge weights). The narrative networks are undirected graphs where the nodes represent our individual narratives and the edges between the nodes represent how often these narratives co-occur with each other. Before drawing the graph, our sentence-level narrative predictions are aggregated to the post level. The nodes in the network graphs are divided into six distinct communities, or clusters. Membership in these communities is determined using k-means clustering. K-means clustering is an unsupervised machine learning technique that finds k number of central locations within the feature space and associates cases, here individual narratives, with these locations (MacQueen 1967).

Finally, we examine textual examples of posts in which military and other frequent narratives co-occur to examine what rhetorical role the military narratives play.

Results

Frequency and Centrality of Military as Key Actant

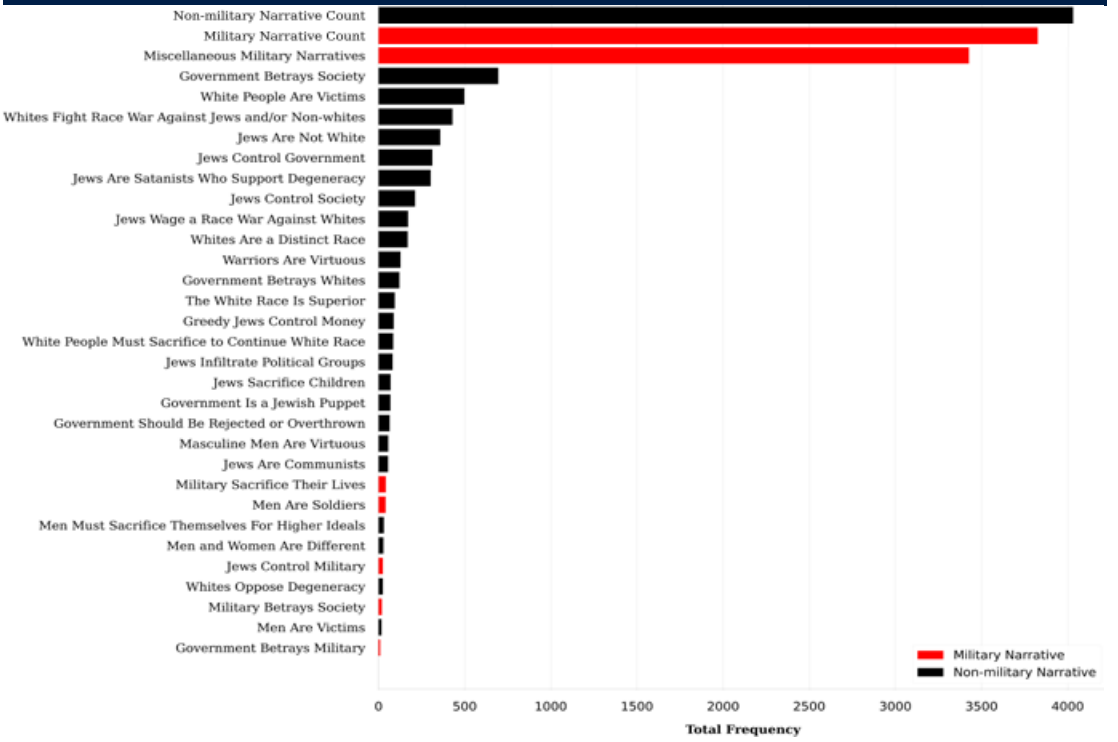
Contrary to our first hypothesis that military actors and narratives will be dominant within the corpus, we find white supremacist content

Table 3. Frequency of Actant Appearance Within Narratives

Supernode	Number of Narratives
Government	19566
Jews	15102
Military	14755
Whites	5649
Men	5091

is more substantial than military content both in terms of the actants and narratives present. Table 3 shows the sentence-level frequency of our main actants. Military represents the third, rather than the first, most frequent group.

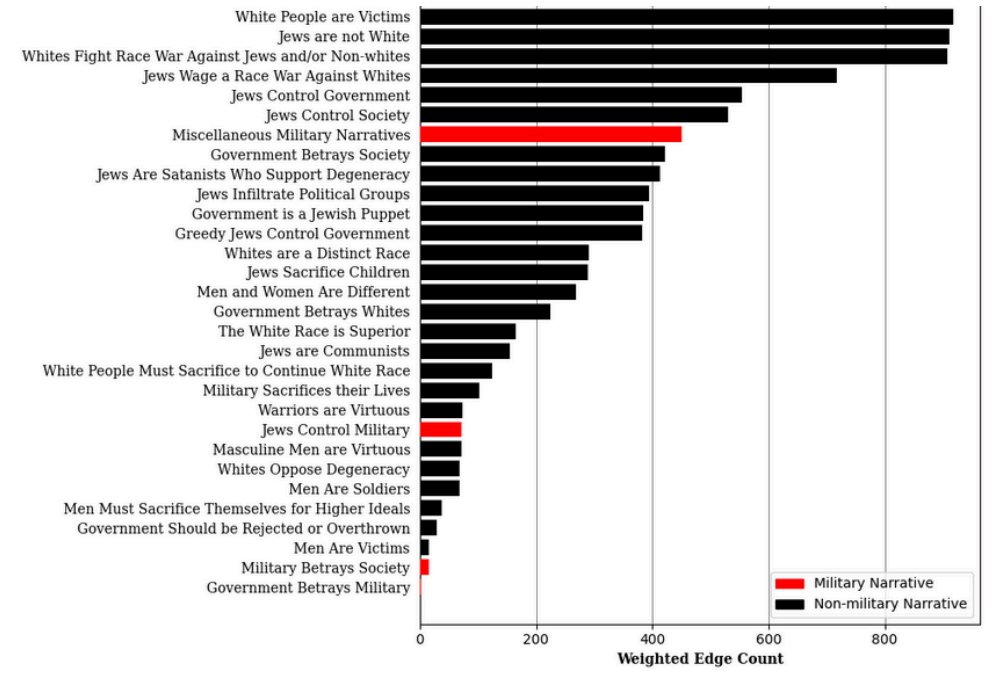
Figure 1. Miscellaneous Military Narratives



Reflecting the frequency of government and Jewish actants, the most common narratives in the dataset deal with white race and antisemitic themes. These include government betrayal, white victimhood, white racial boundaries, and Jewish infiltration of institutions. Military narratives make up less than half of the narratives we observe, and this high representation is largely due to our narrative catch-all, "miscellaneous military narratives."

Contrary to Hypothesis 2 that military narratives will have the highest degree centrality in the network, we find that the most central narratives are not military narratives but are instead narratives about white victimhood, race war, and a variety of antisemitic conspiracy narratives. We calculate degree centrality for each narrative in terms of the total number of edges each narrative shares with each other narrative (displayed in Figure 2). Although many of our military narratives are relatively unconnected to the others, our catch-all for miscellaneous military narratives is in the top quarter in terms of centrality.

Figure 2. Miscellaneous Military Narratives



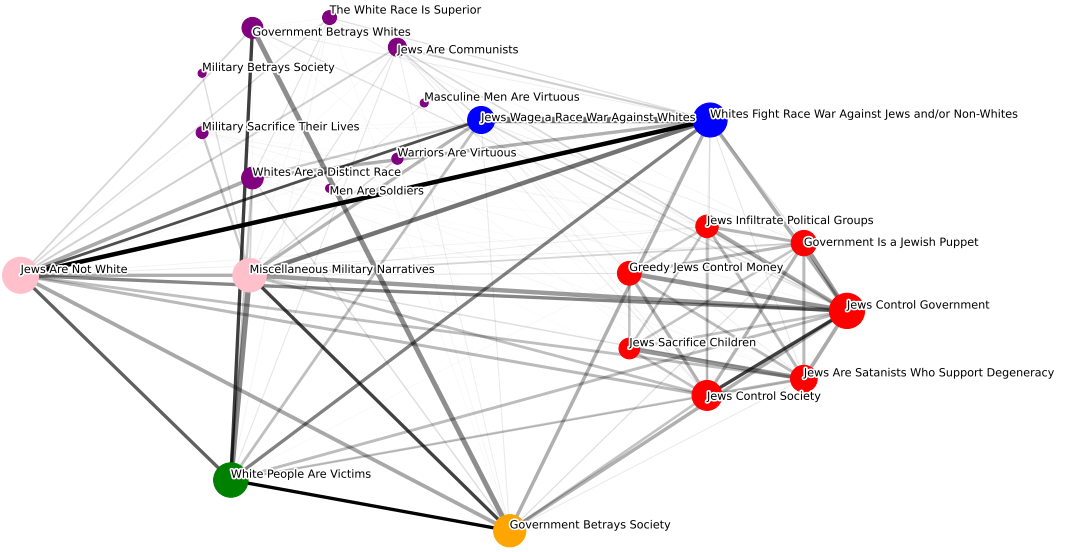
We thus find that, despite selecting on military content for inclusion in our corpus, military narratives do not dominate the corpus but rather are mixed into a larger body of white supremacist narratives. Miscellaneous military narratives are featured far more frequently than any other narratives within the posts, but are less central to the narrative network than white supremacist narratives. In other words, military narratives form the backdrop upon which play out complex compound narratives about white supremacy, government betrayal, and Jewish villainy and control of institutions.

Narrative Network

Our third hypothesis expects that military narratives are embedded within a content network of narratives related to white supremacist concerns, including white victimhood, antisemitic, and anti-government narratives. We see evidence of the role military narratives play in the content network when we examine the network of individual narratives (Figure 3).

Figure 3 shows the narrative network, which is a network where the nodes represent individual narratives and the edges represent the frequency of co-occurrence between two narratives. Overall, we find that 6 communities best represented our data, and the various colors represent different communities of narratives. Two of the communities have obvious substantive significance: the red cluster, which is

Figure 3. Narrative Network



largely a self-involved set of narratives referring to antisemitic conspiracy narratives, and the blue cluster, which contains two reciprocal race war narratives, one with Jews as the protagonist actant and the other with the White Race as the protagonist actant. The pink cluster contains the military narrative "Miscellaneous Military Narratives" and the racial narrative "Jews Are Not White." The green and yellow communities are each defined by a single narrative: "White People are Victims" and "Government Betrays Society," respectively. Finally, the purple community acts as a catch-all, collecting nodes which did not fit into any other cluster. In this community we find low frequency narratives with relatively few edges. These include most of the military narratives, including “Military Betrays Society,” “Warriors are Virtuous,” “Military Sacrifice Their Lives, and “Men are Soldiers,” as well as narratives with Men as an actant and narratives about white superiority.

Along with its co-community member, "Jews Are Not White", "Miscellaneous Military Narratives" forms the dominant conduit between the antisemitic narrative cluster (red) and the rest of the network. "Miscellaneous Military Narratives" also connects strongly to government betrayal narratives—"Government Betrays Society" (yellow) and "Government Betrays Whites" (purple)—which are also primarily connected to the narrative "White People Are Victims" (green). Finally, “Miscellaneous Military Narratives” frequently co-occurs with more specific core military narratives (purple), including “Military Betrays Society, “Warriors are virtuous,” and “Men are Soldiers,” while its co-community member “Jews are Not White” connects to narratives related to white superiority and victimhood: “Government Betrays Whites,”

"Whites are a Distinct Race," "White Race is Superior," and "White People Must Sacrifice to Continue White Race."

In short, within our corpus, military narratives form a primary network pathway leading to narratives concerned with government betrayal, white victimhood and superiority, and antisemitism.

Role of Military Narratives

Finally, our fourth hypothesis is that military narratives are used to heighten the urgency or emotional appeal of the other narratives present in a post. Indeed, we see that this is the case within the corpus. Below we provide two examples. The first contains references to the narratives "Jews Are Not White," "Jews Control Government," and "Miscellaneous Military Narratives." In this case, the military actant is a United States Army Air Corpsman who served in World War II and helped defeat the Nazis. The post refers to the obituary of this veteran, a white man, whose ten-year-old son was sexually assaulted and brutally murdered:

> *.... I found the obituary of the father of the boy listed above. ... "Mr. Fife passed away on September 11, 2006 - exactly twenty-one years to the day that his son, Raymond, died. Mr. Fife was born August 24, 1927, in Weirton, West Virginia, the son of Isaac Danford and Pearl McNurlan. He was a member of the United States Army Air Corps and served in World War II.Mr. Fife was employed at Republic Steel for ten years."*
>
> *A World War 2 vet and a steel worker–and how does Uncle ZOG repay his service to his country? By unleashing the very worst black criminal subhumanity against his family, and then failing to put to death his son's murderers so that both the killers outlived the old man.*
>
> *This is why vigilante violence happens–the people taking the law into their own hands. This white father served the system faithfully during the war, he worked in a steel mill and paid taxes to support the system, and the system pays him back by taking those taxes to provide food, clothing, shelter and medical care to his son's killers so that they may outlive him in prison.*
>
> *A member of the Greatest Generation who helped defeat the Nazis so we could live in the multiracial paradise of today. This is the story of what the Jews and the system have done to white America over the past century. They use them as cannon fodder in their wars, they work them and tax them all their lives, they expose their children to violence, rape and murder by blacks, they give them no justice for what was done to them–then they call them "racist" and say they benefit from a lifetime of "white privilege.*

The author highlights Fife's service to the country and lays out the tragedy of a sacrifice made on behalf of the ungrateful, power-hungry Zionist Occupied Government, or ZOG. Rhetorically, Fife's military service deepens the wrong committed, and further vilifies the alleged perpetrator, embellishing the antisemitic narratives present in the post and adding to the sense of threat.

In another example, we see a wide variety of white supremacist and antisemitic narratives present in a post which also contains our "Miscellaneous Military Narratives," in this case a narrative related to the bombing of Dresden by British fighters during WW2. The post is a rant against Jews, referred to in the post as "your people," accusing them of white genocide and other villainous deeds:

> *...Your people have routinely practiced child sacrifice.*
>
> *Your people have routinely practiced blood libel during passover; the consumption of the blood of children.*
>
> *You murdered Jesus.*
>
> *You enslaved Africans and brought them to the Americas as cheap labour.*
>
> *You constantly practice usury.*
>
> *The governments of UK, US and USSR during WW2 were almost exclusively Jew run which your people used to slaughter over 100 million White's.*
>
> *Jewish run British fighters bombed Dresden, a city with no military installations, killing 600,000 unarmed women and children with fire.*
>
> *Your people and especially your nation drain white nations of wealth.*
>
> *Your people encourage the race mixing of our people, in movies, films, music, from positions of education, power, etc.*
>
> *From positions of political power, Jews braggingly lead the charge in third world immigration to white nations and jail whites who speak against it.*

> **...military narratives make up less than half of the narratives we observe, and this high representation is largely due to our narrative catch-all, "miscellaneous military narratives.**

Here, conspiracy theories about Jewish infiltration of western governments and militaries are heightened by identifying specific battles and incidents of mass casualties—casualties of millions of white people—that are blamed on Jews. Both textual examples show instances of military narratives being combined with white supremacist and antisemitic narratives to heighten the urgency or emotional appeal of these other narratives. In this way, the claims made by the accompanying narrative references (e.g. that whites are victims or that Jews control the government) become exaggerated, and the military narratives contribute rhetorically to a sense of existential threat and high stakes.

Discussion

In this article, we analyze the narrative content of a set of posts from white supremacist chatrooms on Telegram, with an eye to understanding the use of military narratives in these chatrooms and the potential for insider threat related to the military. Despite the narrow focus of our corpus on posts containing military keywords, we find that military narratives play a supporting rather than a leading role in these posts. In aggregate, narratives about the military are not as frequent as narratives about other actants, and individual military narratives are not the most central narratives to the network, which is dominated by narratives about white victimhood, the race war, antisemitic conspiracy narratives, and narratives of government betrayal. Nonetheless, we find that military narratives play an important role within this broader narrative network.

Previous research has suggested that narratives may legitimize violence or hostility against threatening outgroups by reinforcing the ingroup's sense of injury and virtue, while at the same time, emphasizing the evil and danger posed by outgroups (Marcks and Pawelz 2022; Rothbart and Korostelina 2006a; 2006b). A war-like framing of group conflict validates violence as collective self-defense, retribution, or

“

In aggregate, narratives about the military are not as frequent as narratives about other actants, and individual military narratives are not the most central narratives to the network, which is dominated by narratives about white victimhood, the race war, antisemitic conspiracy narratives, and narratives of government betrayal.

even heroism in combating a world-destroying evil (Fiske and Rai 2015; Furlow and Goodall 2011; Marcks and Pawelz 2022). Moreover, would-be warriors of the ingroup are cast as morally responsible for killing and destroying the enemy (Fiske and Rai 2015). Finally, narratives about the military, particularly narratives of soldiers' sacrifice, may be used to impart sacred honor to these warriors and their causes (Dawson and Weinberg 2020). In this study, we find that military narratives play all of these roles within the white supremacist narrative network.

In this study, military narratives serve in the narrative network rhetorically to heighten the stakes of white supremacist narratives contained within the same post. The posts themselves are rarely motivated by their military themes; rather, military narratives serve as background material, lending greater urgency, realism, and gravitas to extremist narratives. The narrative networks in the posts focus on the Jews and the government as key antagonists, the threatening outgroups. Government betrayal narratives connect strongly to narratives of white victimhood. A variety of antisemitic conspiracy narratives in the corpus feature Jews as puppet masters who control government and society. These antisemitic conspiracy narratives connect in the network to narratives of government betrayal and white victimhood but even more strongly to race war narratives, wherein Jews seek to enact white genocide or replacement of the white race. These narrative combinations feature both the language of war and the threat of annihilation. Warrior narratives and narratives of government betrayal of Whites, moreover, combine to depict Whites, especially white men, as noble warriors fighting injustice and the victimization of whites. Furthermore, the separateness of Jews from the white race, a further indication of Jews as the outgroup, is often conveyed in conjunction with stories about the military. These stories are often long-winded and historical in nature, shared with a measure of assumed authority and expertise, serving to provide legitimacy to claims that set Jews apart as a dangerous other. Military narratives are also used to deepen the sense of victimhood or betrayal in accompanying narratives, highlighting unjust military action or unfair treatment of military actors or veterans whose sacrifices deserve honor.

We conclude that far-right chatrooms on Telegram use military narratives to legitimize and heighten the stakes of narratives related to a white supremacist agenda, to vilify Jews, and to glorify violence by warriors for the white race. Military narratives thus becomes part of a rallying cry against outgroups—in this case the Jews and the government—and to heroize warriors for the white race in an effort to recruit and radicalize users to white supremacist causes.

Our findings are limited in that we cannot speak directly to the role of these narratives in the day-to-day recruitment of servicemembers and veterans to extremism. Although we see that white supremacists use military rhetoric to great effect in their own spaces, to what extent military personnel participate in these discussions is unknown. What is also unknown is the generalizability of the particular narrative network we describe to other platforms or audiences. However, the content we observe is well-suited to elicit violence-provoking emotional responses from military audiences and audiences that respect the military.

Our findings have implications for understanding the risk of insider threat related to the military. The use of military language and narratives presents opportunities for insider threat both in relation to recruitment and radicalization of military personnel and veterans and also through the co-option of these narratives in service of extremist causes. In many of the white supremacist Telegram posts, military and government leaders are cast as allies of darkness, at best willing accomplices and at worst the active perpetrators of great crimes against humanity. In contrast, they cast soldiers as victims of manipulation, conspiracy, and betrayal or alternatively as the last bastion against evil forces seeking to annihilate the white race. Lending military honor to extremist causes, these narratives may encourage violence by those who fancy themselves warriors. They may also direct the antipathies of servicemembers and veterans toward government and civilian leaders, creating the dangerous potential for insider threat.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the Institute for Strategic Dialogue for the data used in this paper and Shadi Shahsavari, Pavan Holur, Tianyi Wang, Timothy R. Tangherlini, and Vwani Rochowdhury for their generous provision of code. We thank our colleagues at the New War Research Consortium for the military terms list and for insightful feedback at various stages of this project. Any mistakes are our own. This research was sponsored by United States Military Academy grant W911NF-22-2-0042 and by the United States Air Forces under agreement FA 8650-22-2-6469. The US government is authorized to reproduce and redistribute reprints for Government purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies and endorsements, either expressed or implied, of the United States Air Force, United States Military Academy, or the U.S. Government.

REFERENCES

Chambers, Nathanael, and Dan Jurafsky. 2009. "Unsupervised Learning of Narrative Schemas and Their Participants." In Proceedings of the 47th Annual Meeting of the ACL and the 4th IJCNLP of the AFNLP, 602–10. Suntec. https://aclanthology.org/P09-1068.pdf.

Chermak, Steven, Joshua Freilich, and Michael Suttmoeller. 2013. "The Organizational Dynamics of Far-Right Hate Groups in the United States: Comparing Violent to Nonviolent Organizations." Studies in Conflict & Terrorism 36 (3): 193–218. https://doi.org/10.1080/1057610X.2013.755912.

Cortes, Corinna, and Vladimir Vapnik. 1995. "Support-Vector Networks." Machine Learning 20 (3): 273–97. https://doi.org/10.1007/BF00994018.

Davey, Jacob, and Dana Beth Weinberg. 2021. "Inspiration and Influence: Discussions of the US Military in Extreme Right-Wing Telegram Channels." https://www.isdglobal.org/wp-content/uploads/2021/10/Inspiration-and-Influence1.pdf.

Dawson, Jessica, and Dana Beth Weinberg. 2020. "These Honored Dead: Sacrifice Narratives in the NRA's American Rifleman Magazine." American Journal of Cultural Sociology 10: 110–35. https://doi.org/10.1057/s41290-020-00114-x.

Denbeaux, Mark, and Donna Crawley. 2023. "The January 6 Insurrectionists: Who They Are and What They Did." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4512381.

Devlin, Jacob, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. 2019. "BERT: Pre-Training of Deep Bidirectional Transformers for Language Understanding." arXiv. https://doi.org/10.48550/arXiv.1810.04805.

Fiske, Alan Page, and Tage Shakti Rai. 2015. Virtuous Violence: Hurting and Killing to Create, Sustain, End, and Honor Social Relationships. Kindle iOS. Cambridge: Cambridge University Press.

Flusberg, Stephen J., Teenie Matlock, and Paul H. Thibodeau. 2018. "War Metaphors in Public Discourse." Metaphor and Symbol 33 (1): 1–18. https://doi.org/10.1080/10926488.2018.1407992.

Freilich, Joshua D, Jeremy A Pienik, and Gregory J Howard. 2001. "Toward Comparative Studies of the U.S. Militia Movement." In Varieties of Comparative Criminology, edited by Gregory J Howard and Graeme Newman, 80:163–210. International Studies in Sociology and Social Anthropology. Leiden: Koninklijke Brill NV. https://doi.org/10.1163/9789004473614_009.

Furlow, R. Bennett, and H.L. Goodall. 2011. "The War of Ideas and the Battle of Narratives: A Comparison of Extremist Storytelling Structures." Cultural Studies ↔ Critical Methodologies 11 (3): 215–23. https://doi.org/10.1177/1532708611409530.

Harris, Shane, Samuel Oakford, and Chris Dehganpoor. 2023. "Alleged Leaker Fixated on Guns and Envisioned 'Race War.'" Washington Post, May 13, 2023, sec. National Security. https://www.washingtonpost.com/national-security/2023/05/13/jack-teixeira-discord-leaked-documents/.

Hoffman, Bruce, and Jacob Ware. 2024. "The Urgent Mission to Counter Military Extremism." U.S. News and World Report, January 19, 2024, sec. Commentary. https://www.usnews.com/opinion/articles/2024-01-19/the-urgent-mission-to-counter-military-extremism.

Holthouse, David. 2006. "Several High Profile Racist Extremists Serve in the U.S. Military." Southern Poverty Law Center Intelligence Report, August 11, 2006. https://www.splcenter.org/fighting-hate/intelligence-report/2006/several-high-profile-racist-extremists-serve-us-military.

Lang, Eric L. 2022. "Seven (Science-Based) Commandments for Understanding and Countering Insider Threats." Counter-Insider Threat Research and Practice 1 (1). https://citrap.scholasticahq.com/article/37321.

Lemaître, Guillaume, Fernando Nogueira, and Christos K. Aridas. 2017. "Imbalanced-Learn: A Python Toolbox to Tackle the Curse of Imbalanced Datasets in Machine Learning." Journal of Machine Learning Research 18 (17): 1–5. https://www.jmlr.org/papers/volume18/16-365/16-365.pdf.

Marcks, Holger, and Janina Pawelz. 2022. "From Myths of Victimhood to Fantasies of Violence: How Far-Right Narratives of Imperilment Work." Terrorism and Political Violence 34 (7): 1415–32. https://doi.org/10.1080/09546553.2020.1788544.

McCausland, Jeff. 2019. "Enemies Foreign and Domestic: Inside the U.S. Military's White Supremacy Problem." NBC News (blog). May 25, 2019. https://www.nbcnews.com/think/opinion/inside-u-s-military-s-battle-white-supremacy-far-right-ncna1010221.

Mitchell, Ellen. 2021. "Lawmakers Move to Oust Extremists from Military." The Hill, January 25, 2021." The Hill. https://thehill.com/policy/defense/535503-lawmakers-move-to-oust-extremists-from-military/.

Myre, Greg, and Vanessa Romo. 2019. "Arrested Coast Guard Officer Allegedly Planned Attack 'On A Scale Rarely Seen.'" NPR, February 20, 2019, sec. National. https://www.npr.org/2019/02/20/696470366/arrested-coast-guard-officer-planned-mass-terrorist-attack-on-a-scale-rarely-see.

Pedregosa, Fabian, Gaël Varoquaux, Alexandre Gramfort, Vincent Michel, Bertrand Thirion, Olivier Grisel, Mathieu Blondel, Peter Prettenhofer, Ron Weiss, and Vincent Dubourg. 2011. "Scikit-Learn: Machine Learning in Python." The Journal of Machine Learning Research 12: 2825–30.

Polletta, Francesca. 2008. "Storytelling in Politics." Contexts 7 (4): 26–31. https://doi.org/10.1525/ctx.2008.7.4.26.

Polletta, Francesca, and Jessica Callahan. 2017. "Deep Stories, Nostalgia Narratives, and Fake News: Storytelling in the Trump Era." American Journal of Cultural Sociology 5 (3): 392–408. https://doi.org/10.1057/s41290-017-0037-7.

Ranade, Priyanka, Sanorita Dey, Anupam Joshi, and Tim Finin. 2022. "Computational Understanding of Narratives: A Survey." IEEE Access 10: 101575–94.

Rawnsley, Adam, and Jim LaPorta. 2023. "The Online Racists Stealing Military Secrets." Rolling Stone, April 27, 2023. https://www.rollingstone.com/politics/politics-features/jack-teixiera-case-military-extremism-1234724461/.

REFERENCES

Rothbart, Daniel, and Karina V. Korostelina. 2006a. "Chapter 1 - Introduction: Identity, Morality, and Threat: Studies of Violent Conflict." In Identity, Morality, and Threat: Studies in Violent Conflict, edited by Daniel Rothbart and Karina V. Korostelina, Kindle iOS, 1–17. Plymouth, UK: Lexington Books.

———. 2006b. "Chapter 3 - Moral Denigration of the Other." In Identity, Morality, and Threat: Studies in Violent Conflict, edited by Daniel Rothbart and Karina V. Korostelina, Kindle iOS, 29–58. Lanham: Lexington Books.

Rumelhart, David E., Geoffrey E. Hinton, and Ronald J. Williams. 1986. "Learning Representations by Back-Propagating Errors." Nature 323 (6088): 533–36. https://doi.org/10.1038/323533a0.

Schake, Kori, and Michael Robinson. 2021. "Assessing Civil-Military Relations and the January 6th Capitol Insurrection." Orbis 65 (3): 532–44.

Schnepf, Julia, and Ursula Christmann. 2022. "'It's a War! It's a Battle! It's a Fight!': Do Militaristic Metaphors Increase People's Threat Perceptions and Support for COVID-19 Policies?" International Journal of Psychology 57 (1): 107–26. https://doi.org/10.1002/ijop.12797.

Schrama, Michael. 2023. "Creating a Codified Legal Response to Domestic Extremism in the Ranks." War on the Rocks (blog). July 19, 2023. https://warontherocks.com/2023/07/creating-a-codified-legal-response-to-domestic-extremism-in-the-ranks/.

Schulze, Heidi, Julian Hohner, Simon Greipl, Maximilian Girgnhuber, Isabell Desta, and Diana Rieger. 2022. "Far-Right Conspiracy Groups on Fringe Platforms: A Longitudinal Analysis of Radicalization Dynamics on Telegram." Convergence 28 (4): 1103–26. https://doi.org/10.1177/13548565221104977.

Shahsavari, Shadi, Pavan Holur, Tianyi Wang, Timothy R. Tangherlini, and Vwani Roychowdhury. 2020. "Conspiracy in the Time of Corona: Automatic Detection of Emerging COVID-19 Conspiracy Theories in Social Media and the News." Journal of Computational Social Science 3 (2): 279–317. https://doi.org/10.1007/s42001-020-00086-5.

Simi, Pete, Bryan F. Bubolz, and Ann Hardman. 2013. "Military Experience, Identity Discrepancies, and Far Right Terrorism: An Exploratory Analysis." Studies in Conflict & Terrorism 36 (8): 654–71. https://doi.org/10.1080/1057610X.2013.802976.

Smith, Brent L., Andrew J. Bringuel II, Steven M. Chermak, Kelly R. Damphousse, and Freilich, Joshua D. 2011. "Right-Wing Extremism and Military Service." In Terrorism Research and Analysis Project (TRAP): A Collection of Research Ideas, Thoughts, and Perspectives, edited by Andrew Bringuel, Jenelle Janowicz, Abelardo Valida, and Edna Reid, 1:341–64. Washington, D.C.: Department of Justice, Federal Bureau of Investigation. https://www.tandfonline.com/doi/abs/10.1080/1057610X.2013.802976.

Smith, Philip. 2005. Why War?: The Cultural Logic of Iraq, the Gulf War, and Suez. 1st ed. Chicago: University of Chicago Press.

Stafford, Kat, and James LaPorta. 2021. "Decades of DOD Efforts Fail to Stamp out Bias, Extremism." AP News. https://apnews.com/article/business-donald-trump-lloyd-austin-veterans-arrests-aa564fe473dd4c347189bb39ad8a9201.

Tangherlini, Timothy R., Shadi Shahsavari, Behnam Shahbazi, Ehsan Ebrahimzadeh, and Vwani Roychowdhury. 2020. "An Automated Pipeline for the Discovery of Conspiracy and Conspiracy Theory Narrative Frameworks: Bridgegate, Pizzagate and Storytelling on the Web." PLoS ONE 15 (6). https://doi.org/10.1371/journal.pone.0233879.

Urman, Aleksandra, and Stefan Katz. 2022. "What They Do in the Shadows: Examining the Far-Right Networks on Telegram." Information, Communication & Society 25 (7): 904–23. https://doi.org/10.1080/1369118X.2020.1803946.

U.S. Department of Justice Office for Public Affairs. 2020. "Press Release: U.S. Army Soldier Charged with Terrorism Offenses for Planning Deadly Ambush on Service Members in His Unit." U.S. Department of Justice Office for Public Affairs. June 22, 2020. https://www.justice.gov/opa/pr/us-army-soldier-charged-terrorism-offenses-planning-deadly-ambush-service-members-his-unit.

———. 2023. "Press Release: Air National Guardsman Indicted for Unlawful Disclosure of Classified National Defense Information." U.S. Department of Justice Office for Public Affairs. June 15, 2023. https://www.justice.gov/opa/pr/air-national-guardsman-indicted-unlawful-disclosure-classified-national-defense-information.

Ware, Jacob. 2023. "The Violent Far-Right Terrorist Threat to the U.S. Military." Council on Foreign Relations, January 31, 2023. https://www.cfr.org/blog/violent-far-right-terrorist-threat-us-military.

Weinberg, Dana Beth, and Jessica Dawson. 2021. "From Anti-Vaxxer Moms to Militia Men: Influence Operations, Narrative Weaponization, and the Fracturing of American Identity." The Brookings Institute. https://doi.org/10.31235/osf.io/87zmk.

Weinberg, Dana Beth, Jessica Dawson, and April Edwards. 2022. "How the Russian Influence Operation on Twitter Weaponized Military Narratives." Proceedings of the 18th International Conference on Cyber Warfare and Security (ICCWS) 18 (1): 431–39. https://doi.org/10.34190/iccws.18.1.985.

Wolf, Thomas, Lysandre Debut, Victor Sanh, Julien Chaumond, Clement Delangue, Anthony Moi, Pierric Cistac, et al. 2020. "Transformers: State-of-the-Art Natural Language Processing." In Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing: System Demonstrations, 38–45. Online. https://aclanthology.org/2020.emnlp-demos.6.

LESSONS LEARNED AND CASE STUDIES

Safeguarding Psychological Safety in a High Performing Organization

Shari S. Bowen, DM
Lidilia AmadorGarcia, MS

The conversation of managing insider risks and organizational resilience is a timeless concept, central to leadership discussions within organizations of every type. Building awareness of such qualitative challenges as individual concerns, discomforts, and offenses enables early risk identification within an organization. Human discomfort within an organization creates a welcome environment for threat activity endangering the organization and/or its members. The discomfort that serves as a source of the risk may originate from a non-inclusive system, a broken process, or a new requirement.

SHARI S. BOWEN

Dr. Shari Bowen is an Assistant Professor at the United States Military Academy with over 25 years of experience in leading within organizations, to include not for profit, where leadership is voluntary. Dr. Bowen's educational areas of focus are Organizational Psychology and Organizational Leadership. Her interests lie in the effects of leadership to organizational behaviors. Dr. Bowen focuses on enhancing academia through use of case studies and quick cases to inform this generation of learners.

Early identification of such potential risk and threat vectors facilitates mitigation, however leaders may be hesitant to recognize the existence of personal discomforts among their employees. This case explores a possible source of discomfort created by an organizational leader that heightens the risk for insider threat. It further explores the human psychological processes an individual can experience as daily behaviors facilitate an environment for insider threats to thrive. While psychological safety impacts and enables dynamic environments within an organization, lack of psychological safely does the opposite, presenting risks that lead to insider threats. The following case is based on actual events, exploring how normal daily actions can present increased risk within a high functioning organization.

Professor Jackson was honored to accept a teaching position at one of the nation's most renowned universities. She cherished the opportunity to share her lifetime of knowledge and experiences to "give back" by contributing to the next generation's education. As she arrived at the new job, she was given an overview of the hierarchy and managerial structure within the organization. Management within Professor Jackson's department included the Department Chair, Department Executive Assistant (EA), Program Coordinators (PC), Program EA, and Faculty. In addition to serving as faculty, Professor Jackson had the responsibilities of serving as Program EA. Her duties and responsibilities included: program synchronization meetings, planning and resourcing, coordinating with visitors, syllabus maintenance for the program and its courses, scheduling, and managing other miscellaneous administrative functions. Professor Jackson's Program Coordinator established clear expectations and requirements.

LIDILIA AMADORGARCIA, MS

Major Lidilia AmadorGarcia is an AMEDD Captain Career Course Instructor with over 25 years of leadership experience. Major AmadorGarcia's educational areas of focus are marriage and family and leadership. Her interests lie in the effects of psychology on leadership. Major AmadorGarcia focuses on enhancing academia through mentorship, recruitment, and retention.

After a few months on the job, things seemed to be going well. Based on informal conversations with her Program Coordinator, Professor Jackson believed the semester to be progressing as it should. The two exercised open conversation to alleviate the need for assumptions. The PC consistently made small talk and said things like, "thank you for all you do… I'm hearing great things about you." There were no complaints. The Program Coordinator led a discussion at the end of the academic semester about communication within the program and indicated that Professor Jackson was meeting expectations. Professor Jackson believed that she garnered the momentum needed to continue to excel in the next academic semester. Robbins and Judge (2019) discuss five functions of communication within an organization: management, feedback, emotional sharing, persuasion, and information exchange factors. Of the five, management serves the purpose of managing the behavior of the people involved in the communication (Robbins and Judge, 2019). Up to this point, open communication fostered transparency, feedback, and information exchange without apprehension.

One day, prior to the program synchronization meeting that Professor Jackson was to facilitate, the PC abruptly informed her in passing, that a new position had been created within the program, that it would be announced at the meeting, and the fair-

> **"Human discomfort within an organization creates a welcome environment for threat activity endangering the organization and/or its members.**

ly new (2 months on ground) hire would facilitate the meeting. How could a new hire facilitate the meeting… "her meeting?" Her immediate feelings were confusion and rejection. Professor Jackson felt blindsided. Her immediate perception was that the new position seemed to have overlapping duties and responsibilities with her own. The value of effective communication impacts attitudes and behavior outcomes. Researchers indicate there are three major aspects to attitudes: affect, 2, 3. The affect component is most known to impact individual behaviors within an organization (Robbins and Judge, 2019). When paired with the cognitive component it leads to actions carried out in the behavioral component (Robbins and Judge, 2019). The complexity of our individual attitudes lends to a multitude of reasons why leaders within organizations should create psychological safety. It also establishes an explains how an insider threat can begin within an organization. Attitudes directly impact the level of commitment, or lack thereof (Robbins and Judge, 2019).

Rather than creating tension in the office, the professor accepted the change, despite knowing no other program had a similar position. As a Program EA, Professor Jackson felt her performance must be substandard, otherwise this new position would not have been resourced. As Professor Jackson worked to organize the experience and assign a proper perception, she openly processed her feelings. She was disappointed that her leader did not have a direct conversation with her about the gap between expectations and her performance. Professor Jackson felt professionally devalued because her leader did not discuss the advent of a new position that seemed to overlap with her published responsibilities prior to a meeting where someone else was executing her assigned tasks. Although all communication seemed to point to success, the PC's actions seemed to indicate failure, leaving Professor Jackson confused and upset.

Professor Jackson internalized her sentiments although it bothered her. She tried to rationalize why this decision was made and assess the situation from multiple perspectives. The decision created a climate in which Professor Jackson believed she could not communicate her concerns with her supervisor. She felt isolated. Department and program supervisors had (perhaps unknowingly) created an environment where it was difficult for a valued teammate to address legitimate concerns. To not

"

…supervisors had (perhaps unknowingly) created an environment where it was difficult for a valued teammate to address legitimate concerns.

"rock the boat," Professor Jackson accepted the decisions made, while considering the proper manner to address a situation that led to her own internal turmoil.

The insider threat began with communication, which started well, but was doubted once the leader actions did not align. The EA's attitude was impacted, directly impacting her perception. This poses a problem and drives an individual to decide. Should Professor Jackson address the issue with her Program Coordinator? A decision is necessary when there is a discrepancy between the way things are and the desired end state (Robbins and Judge, 2019).

A psychologically safe environment fosters individual and holistic learning for the team (Brassey et al., 2022). Amy Edmondson introduces this idea of psychological safety, explaining psychologically safe environments make space for interpersonal risk-taking (Brassey et al., 2022). In the new environment, Professor Jackson was not comfortable she could take such risks. She now experienced anxiety about how to address the problem, ambiguity about her feelings and the truth, and apprehension to even speak about the situation. She had become conditioned to believe (based on past organizational experiences), if a boss created a new position with overlapping responsibilities, that boss does not appreciate her level of competence or performance.

Professor Jackson considered this new environment. Was the problem Professor Jackon's lack of proficiency or her boss' lack of authenticity and ability to have a difficult conversation? Angered and disappointed, she talked about the actions of work at home. She could continue accepting the climate in which she operated, or she could approach the boss with open communication.

Professor Jackson decided she needed to be courageous and work to address the uncertainties she felt. After a few weeks and hearing other leaders within the organization speak, she felt as though the department truly valued excellence. She considered the possible intentions of the PC's actions and decided it was appropriate to have a discussion. Preparing for this discussion Professor Jackson carefully considered her approach, the implications of her role in an environment where she was in the minority, and how to relate the facts as she experienced them... If this situation was not handled appropriately, or received well, it could negatively impact her job security.

Though Professor Jackson was offended by the decision to create a new position which overlapped her role, she felt she owed the organization her perspective and a true assessment. If this high performing organization truly prided themselves on cohesion and team effectiveness, as she had heard through other discussions, what was happening in this situation? There was a new teammate socialized into the new culture, who was feeling overlooked, bypassed, replaced, devalued, disrespected... Someone needed to know this.

> **Many high performing organizations continue to possess fertile ground for insider threats, that begin with, and can end with basic leadership skills.**

Professor Jackson did not like the feelings of disgruntlement she was beginning to feel toward her leadership and even the institution, which she so highly regarded. Effective communication, active listening, clear articulation, non-emotional responses, were a few necessities to an effective conversation. Professor Jackson called for the meeting. She was relieved to know her PC's intent was not to make a change disregarding impact to the EA. The PC agreed, she could have used a better method and more effective communication to get the desired results. The important lesson was communicated. The truth Professor Jackson came to terms with, was that the intent of the leader did not alleviate the feelings she was experiencing. Though she was a little more at ease after hearing the intent of the PC yet found it important to reenforce the perception given from micro aggressive behavior. Microaggressions, took insider threat to another level. Based on Professor Jackson's demographics, there were considerations about race she thought of, that added a layer to her attribution, impacting the way she perceived the situation (Robbins and Judge, 2019). She shared the importance of awareness between leader and subordinate. She spoke about the impacts of the power dynamic in a supervisor - follower relationship, and difficulty to speak up in a new environment. The conversation was fruitful and strengthened the program. The lessons learned from the experience assisted with modifying the decision-making process immediately, strengthening the psychological safety within the department (Brassey et al., 2022).

Upton and Creese (2014) discuss organizations that have a probability of experiencing insider threats tend to minimize the impact of the threats, assuming the members of the organization are safe from internal threats and channel resources to protect from external threats (Upton et al., 2014). Extending that idea, a prevailing notion is that individuals within the organization are "teammates" and cannot or would not be harmed by each other. This case offers the opportunity to read and apply proper decision-making to an act which occurs more often than we realize daily in high performing organizations.

Human discomfort provides a risk for insider threat within an organization. The insider threat is further exacerbated when there is a lack of psychological safety, whether actual or perceived. Professor Jackson found the courage to speak up. There are individuals whose discomfort is never addressed. This case allows us to understand leaders must develop an appetite for the well-being of employees and the necessity for difficult conversations which have great bearing on these uneasy feelings. Effective communication can be difficult. Social anxiety, and cross-cultural barriers give cause for adding layers of difficulty to communication (Robbins and Judge, 2019). Effective communication and difficult conversations help promote an environment of psychological safety and open a door for employees to facilitate improved group dynamics, build effective teams, improve work motivation, and address needed changes.

Professor Jackson was in a situation where individual negative feelings about the organization could have festered and manifested in further negative behaviors. Many high performing organizations continue to possess fertile ground for insider threats, that begin with, and can end with basic leadership skills. Training leaders to increase awareness prevents employees from toiling with the attitudes, cognitions, and behaviors alone. In summary, there is a way to create an environment that decreases probability of insider threat by applying basic leadership skills. Based on the lived experience of Professor Jackson, a method that enhanced psychological safety in an already high performing organization consisted of the behaviors below. It increased the divide between insider threats and organizations:

- Leader authenticity
- Alignment of speech and actions
- Setting clear expectations
- Informal confidence checks
- Formal quarterly reviews
- A climate of open communication
- A climate that welcomes and facilitates difficult conversations with no retaliation,
- Supervisor active listening engagements with employees.

DISCLAIMER

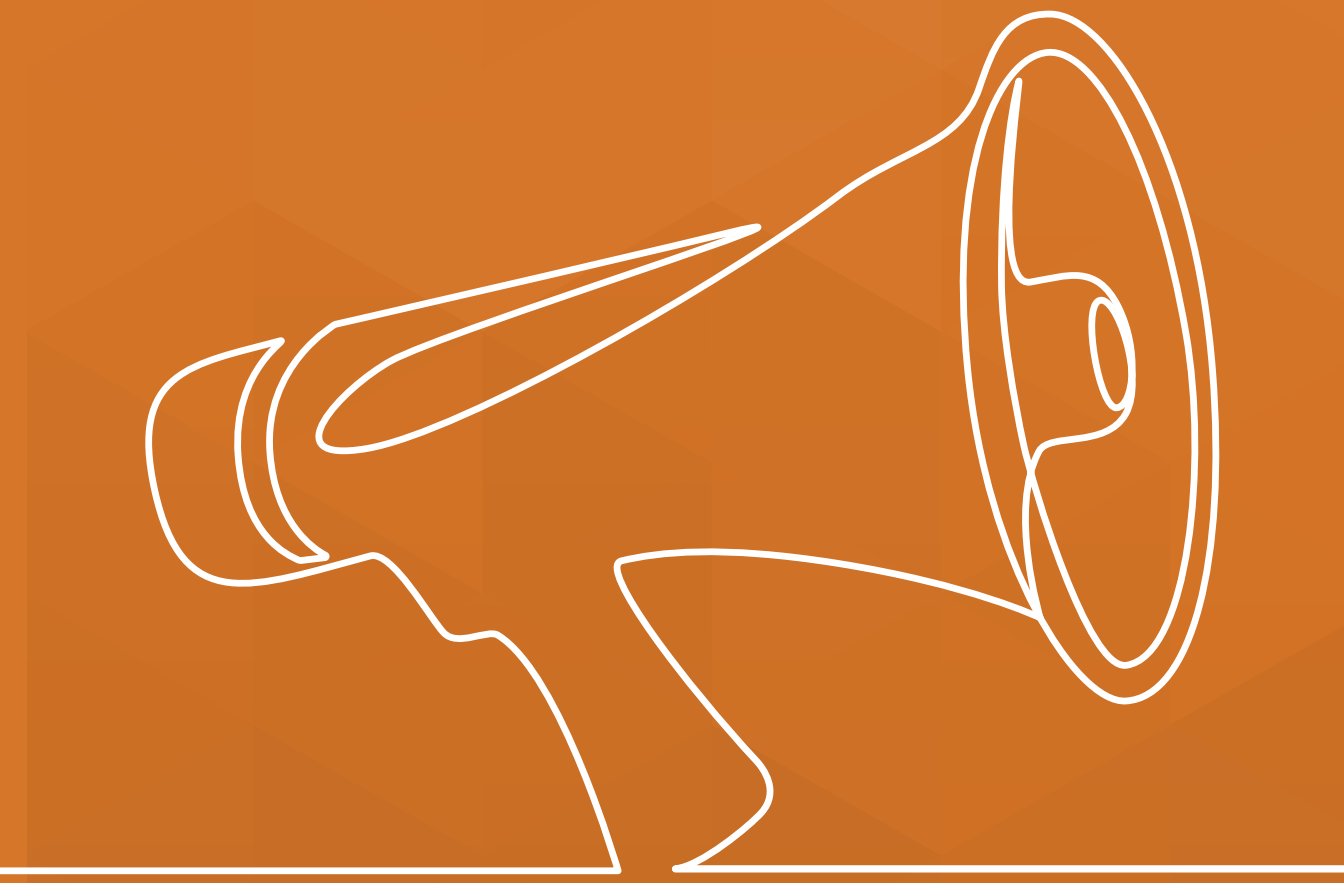
The information and views expressed in this presentation are solely those of the author and do not represent opinions and policies of the Department of Defense, U.S. Government, U.S. Special Operations Command, the Joint Special Operations University, or the institutions with which the author is affiliated.

REFERENCES

Amy, Edmondson, C. 2018. The Fearless Organization. New York, NY: John Wiley & Sons.

George Silowash, Dawn Cappelli, Andrew P. Moore, Randall f. Trzeciak, Timothy Shimeall, and Lori Flynn. "Common sense guide to mitigating insider threats." (2012).

Stephen P. Robbins and Timothy A. Judge. 2019. *Organizational Behavior*, 18th Edition. Pearson. Pg. 357.



SUBMISSIONS AND CALL FOR PAPERS

Submissions and Call for papers

The MIROR JOURNAL
Managing Insider Risk and Organizational Resilience

EDITOR-IN-CHIEF
Jonathan W. Roginski, Ph.D.

CONTACT
jonathan.roginski@westpoint.edu
insiderthreat@westpoint.edu

MANUSCRIPT SUBMISSIONS
https://www.editorialmanager.com/mirorjournal/default2.aspx

Managing Insider Risk and Organizational Resilience (MIROR) Journal is an editorial-reviewed online and print publication. MIROR will share research, best operational practices, leadership perspectives, and reviews of relevant work that further both the proactive practices of insider risk management and promotion of holistic wellness and resilience in organizations.

The editors will review content across those areas that move discussion forward concerning insider risk and organizational resilience, including but not limited to the following:

- **Recruitment and pre-employment screening.** How do we recruit and hire the right "fit" for our organization, facilitating higher performance and better retention?
- **Development and/or implementation of policies and practices.** How does an agency build policies and practices to accomplish its mission while maximally protecting against risks presented to mission accomplishment from the inside?
- **Training and education.** How do we effectively train the workforce on policies and practices (prepare for the known) and educate toward continuous improvement (prepare for the unknown)?
- **Continuous evaluation.** How do we foster trust across the enterprise by thoughtfully and respectfully verifying the alignment of values between individual and organization extant at hiring continues to result in mutually supportive behaviors?

- **Risk modeling and reporting.** How do we leverage the suite of quantitative and qualitative mathematical, statistical, and mental models that exist (or will exist) against the challenge of keeping people and organizations happy, healthy, and safe? How are the results of those models communicated to leaders to facilitate decision making and change?
- **Data science applications.** Data science is arguably the most "in-demand" contemporary analytical field—how may we benefit from the groundbreaking knowledge and techniques in the insider risk and threat management field?
- **Creation and maintenance of positive organizational culture.** Employees that are connected to and invested in their organization and feel reciprocity from the company are protective and constructive toward themselves, their peers, and the company. How do we make, keep, and foster such an environment?
- **Employee intervention.** Identify people and practices that increase risk of negative insider activity and align appropriate resources to protect people and the enterprise?

ARTICLE TYPES AND SUBMISSION

Submissions in the following categories are welcome:

Professional Commentary (800+ words) Professional commentaries seek to bring forward insight from leaders in the field and highlight recent developments, concerns, and bridge gaps between industry, government, and academia. A Professional Commentary includes references as embedded discussions in the text and no endnotes.

Traditional Research Article (up to 5,000 words) with findings and results.

Research Notes are short articles (1500 – 2500 words) with preliminary findings, early results, or responses to current developments. Endnotes must be hyperlinked with the text referenced. Discursive endnotes are strongly discouraged; cite only direct quotations and paraphrases. No need for a bibliography. The journal's formatting style is the Chicago Manual of Style (CMS), 17th edition, endnotes.

Lessons Learned, Case Studies, Vignettes (500 – 1500 words) Experiences from practitioners and professionals close to the developments in the field. The article type is a feedback loop from the field back to the community. A Lessons Learned, Case Studies, Vignettes article has needed references as embedded discussions in the text and no endnotes.

Review Article (1000 – 2000 words) Synthesize seminal and/or canonical works in a particular area informing the ideas of insider risk and organizational resilience to inform the readership of important foundational knowledge in the field.

Book Review (1000 words) Traditional academic book review with no endnote references.

The HQDA G-3/5/7, DAMO-ODP, Army Counter-Insider Threat Program is an integrated effort across the Total Army established to protect installations, networks, facilities, personnel, and missions from the risk insiders pose to national security.

U.S. ARMY

COUNTER-INSIDER THREAT PROGRAM

HQDA | DCS | G-3/5/7 | DAMO-ODP/DAMO-ODH

From the offsite contractor logically accessing Army networks to the senior Army leader stationed on the Pentagon Reserve, and Soldiers, staff, and personnel everywhere in between, the Army Counter-Insider Threat Program develops policies and procedures to improve the Army's reaction and pre-emptive responses to combat risks posed by existing and evolving threats.

The **Army Counter-Insider Threat Program Management Team** consists of highly trained individuals focused on policy development training and awareness, reporting procedures, and data processing to continually enable all Army Commands, Army Service Component Commands, and Direct Reporting Units to prevent, deter, detect, and mitigate insider threats.

For questions or for more information about the Army Counter-Insider Threat Program please contact the organizational inbox:

usarmy.pentagon.hqda-dcs-g-3-5-7.mbx.damo-odp-counter-int@army.mil.

the ThreatLab

Integrating Research Into Practice

The insider threat is a human problem resulting from a complex interaction among individuals and environmental factors.

Social and behavioral sciences are well-suited to address this complicated and persistent human problem.

The Defense Personnel and Security Research Center founded the Threat Lab in 2018 to incorporate the social and behavioral sciences into the counter-insider threat mission space. Our vision is to be a global leader in creating and sharing social and behavioral sciences knowledge to counter the insider threat.

- We work with stakeholders to transform operational challenges into actionable research questions.
- We design and execute research projects that result in accessible, concise findings and recommendations
- We integrate into training and awareness materials that organizations can use or customize for their own purposes.

The Threat Lab portfolio includes exploratory research, professionalization (education, training, certification and tradecraft programs) and outreach activities.

The West Point Insider Threat Program connects Department of Defense and Department of the Army's Insider Threat efforts with an interdisciplinary team to counter insider threat by fostering a positive leadership climate that reduces threat likelihood and impact.

When the Office of the Under Secretary of Defense (I&S) and the Department of Army recognized a need; the US Military Academy and Department of Mathematical Science answered the call. The result is the Insider Threat Program which builds an ecosystem of trust, development, and caring to create an environment incompatible with Insider or Inside Threat.

Change the conversation about Insider Threat

- Why does Insider Threat happen?
- How do we prevent?
- How do we detect?
- How do we mitigate effects?

Support to DoD and Army

- Oath to Constitution
- Army Prioritized Protection List
- Network Engagement Team

Deploy Artifacts

- Undergraduate internships, presentations, theses
- MIROR Journal

For inquiries and information about West Point Insider Threat Program
email: insiderthreat@westpoint.edu
web: insiderthreat.westpoint.edu

The MIROR JOURNAL
Managing Insider Risk and Organizational Resilience