



INSTITUTE FOR DEFENSE ANALYSES

Study on Cyberexploitation and Online Deception of Members of the Armed Forces and Their Families – Public Version

Thomas M. Kelso, Project Leader

Jordan A. Adams-Leavitt

Michelle G. Albert

Sujeeta B. Bhatt

Scott Cunningham

Shane Gillies

Janna R. Mantua

Ian W. McDaniel

Alexander Rios

Allison J. Savoy-Logan

Grace H. Spinner

October 2023

Distribution Statement A.
Approved for public release:
distribution is unlimited.

IDA Product 3001914

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305



The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-19-D-0001, Project BC-5-5196, "Cyberexploitation of Members of the Armed Forces and their Families," for the Office of the Secretary of Defense (OSD), Deputy Chief Information Officer for Resources and Analysis. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgements

Scott Schutzmeister, Laura A. Odell

For More Information

Thomas M. Kelso, Project Leader
tkelso@ida.org, 703-845-2486

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Copyright Notice

© 2023 Institute for Defense Analyses
730 East Glebe Road, Alexandria, Virginia 22305 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (Feb. 2014).

Executive Summary

Introduction

The Department of Defense's (DoD's) Deputy Chief Information Officer for Resources and Analysis tasked the Institute for Defense Analyses (IDA) to conduct a study on the cyberexploitation and online deception of members of the Armed Forces and their families. The task originated in Section 589F of the 2021 National Defense Authorization Act (NDAA), which directed the Secretary of Defense to conduct the study and to provide a report to the Committees on Armed Services of the House of Representatives and the Senate.¹

Per Section 589F of the 2021 NDAA,² *cyberexploitation* “means the use of digital means and online platforms (A) to knowingly access, or conspire to access, without authorization, an individual's personal information to be employed (or to be used) with malicious intent; or to deceive an individual with misinformation with malicious intent; or (B) to deceive an individual with misinformation with malicious intent.” The NDAA language requested assessments and analyses of predatory loans, financial products, and educational products; unproven or unnecessary medical treatments or procedures; ethnic or racial violent extremist messages; social media algorithms; intelligence assessments of threats from foreign government and non-state actors; case studies; DoD actions to educate members and their families; and recommendations for changes to policy and legislative action.

Predatory Loans

Predatory lending occurs “when a lender uses unfair or deceptive tactics to lead a borrower into taking a loan that carries terms that benefit the lender at the borrower’s expense.”³ Types of predatory loans include payday loans, car title loans, and installment loans. Service members are targeted with deceptive practices and are prone to exploitation for several reasons, including demographics, the military lifestyle of frequent moves and deployments, and the military culture of readiness. The DoD defines financial readiness as, “the state in which successful management of personal financial responsibilities supports a servicemember’s ability to perform their wartime responsibilities.”⁴ In addition, service members and veterans are often targeted and exploited by

¹ The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 116th Cong. Pub. L. 116-283, January 1, 2021.

² Ibid.

³ <https://www.nerdwallet.com/article/loans/personal-loans/what-is-predatory-lending>

⁴ Congressional Research Service R46983, *Military Families and Financial Readiness*, preface.

for-profit schools using affinity marketing in a deceptive manner, via online or hardcopy marketing materials, as well as through the use of aggressive recruiters or marketers. Predatory lending and those related practices associated with educational products can have serious personal and professional ramifications for the affected service member, which may in turn negatively affect his or her unit.

Unnecessary or Unproven Medical Treatments

Social media is the primary threat vector for cyber-related targeting using unproven or unnecessary medical treatments or procedures. Service members and their families often use social media as a means of entertainment, learning, and connection as they move from duty station to duty station. Spouses of service members are especially reliant on social media, as they often face challenges finding employment in new locations. This makes both service members and their families susceptible to direct selling or multi-level marketing (MLM) schemes involving health products as a means of earning additional income.

Racially and Ethnically Motivated Violent Extremist Messages

Despite significant differences in their meanings, radicalization, extremism, and terrorism have been often (and incorrectly) used interchangeably to describe violent action taken in support of an extremist ideology or motivation. *Extremism* refers to ideologies, beliefs, and convictions that are considered to be on the fringes of the fundamental values of society and democracy, such as beliefs that often advocate the supremacy of a particular group (racial, religious, political, economic, social, etc.). *Radicalization* is a dynamic, multi-stage, multi-faced cognitive and behavioral process that differs for each individual, as radicalization is influenced by a number of factors (i.e., there is no single pathway or explanatory theory for radicalization that applies to all individuals or groups).⁵ Though previous studies have not supported the idea that service members are more vulnerable to extremist radicalization than their civilian counterparts, interviews with current and former members of far right, White supremacist, and hate groups revealed that the need for belonging was a common motivator for active-duty and veteran service members to join extremist organizations.⁶ Although there is currently no open source evidence that extremist organizations have turned to the use of deepfakes for recruitment and radicalization of service members and their families, a two-year investigation by the Vietnam Veterans of America (VVA)

⁵ R. Borum, *Psychology of Terrorism*, (. Tampa, FL: University of South Florida, 2004); R. Borum, “Radicalization in Violent Extremism I: A Review of Social Science Theories,” *Journal of Strategic Security* 4, no. (4 (2011): 7–36.

⁶ Helmus, Todd; Brown, Ryan Andrew; & Ramchand, Rajeev. (2023). Prevalence of Veteran Support for Extremist Groups and Extremist Beliefs: Results from a Nationally Representative Survey of the U.S. Veteran Community. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1071-2.html.

found a “persistent, pervasive, and coordinated online targeting of American servicemembers, veterans, and their families by foreign entities who seek to disrupt American democracy.”⁷

Sextortion

Sexual extortion, or sextortion, occurs when a victim is approached online by a perpetrator who threatens to expose the victim’s intimate information if the victim does not pay a specified sum of money. In some cases, the perpetrator’s threats are predicated upon bluffs that they possess intimate images or videos of the victim. In other cases, the perpetrator genuinely does have access to intimate images or videos of the victim that they can choose to expose if the ransom is not paid. These cybercriminal operations are relatively easy to conduct, even with few resources or computer skills. Recently, young Americans have become increasingly vulnerable to online sexual scams. This demographic is the same as thousands of current and future U.S. service members and is illustrative of their vulnerability to online scams of a sexual nature, a vulnerability that cybercriminals are actively exploiting. Beyond the financial and mental welfare damage, sextortion of service members also poses a national security risk. The advancement of machine-manipulated media (i.e., deepfakes) has resulted in increased online sexual harassment and extortion. It is likely that such an evolution in cybercriminal strategy will be increasingly successful at targeting women in the military

Machine Manipulated Media (or “Deepfakes”)

Deepfakes are realistic photo, audio, video, and other forgeries generated with artificial intelligence (AI) technologies.⁸ Deepfake content was originally created by a form of AI called generative adversarial networks (GANs). Variational autoencoders are a generative AI model that have been used in text-to-image platforms. Stable diffusion is a newer text-to-image technology that includes components of variational autoencoders. When deepfakes entered the mainstream, they were expensive and arduous to create. However, there is now a lower barrier of entry for creating deepfakes and a growing number of examples of deepfakes being used for nefarious purposes. In a number of cases, nation-states have used deepfakes to create the persona of a rival national figure in an attempt to achieve their objectives. Deepfakes have predominantly been used against the general public to make “traditional” types of scams more convincing. The greatest current deepfake threat in the DoD is against senior leaders (i.e., general officers, senior executives). Senior leaders are public-facing individuals who often have pictures and videos in the public domain, and it is easy to use their face or voice to create deepfakes. The proliferation of deepfake content presents a broader problem — a general disbelief in information. In a “post-truth

⁷ Kristofer Goldsmith, *An Investigation into Foreign Entities Who Are Targeting Servicemembers and Veterans Online*, Vietnam Veterans of America, 2019. <https://vva.org/wp-content/uploads/2019/09/VVA-Investigation.pdf>.

⁸ Congressional Research Service, “Deep Fakes and National Security”, April 17, 2023, <https://crsreports.congress.gov/product/pdf/IF/IF11333/7>

society,” misinformation and disinformation are rampant, and manipulation tactics, such as deepfakes, can be used to amplify false narratives.

National Intelligence Assessments

The National Intelligence Priorities Framework (NIPF) is a hierarchy designed to maximize the efforts of a finite IC workforce and other resources to address a nearly unlimited range of topics central to national security. Although the specifics are classified, Intelligence Community Directive (ICD) 204 states “The NIPF provides the mechanism for the development and communication of overarching national intelligence priorities and the evaluation of IC responsiveness and progress against those priorities.” Further, “National Intelligence priorities shall reflect consideration of the value of intelligence activities to U.S. national interests and the risks entailed in the potential exposure of intelligence priorities.”⁹ A process exists to allow IC Functional Managers to make ad hoc updates to the priorities to generate greater targeting, collection, processing, exploitation analysis and dissemination of intelligence on any topic, especially across “seam” issues like cyberexploitation.

While not officially defined within Joint Force doctrine, information warfare (IW) “encompasses the range of offensive and defensive efforts that use information across the competition continuum to exploit the information environment against adversaries, to inform public opinion, and to compel decision makers to take certain actions.”¹⁰ Objectively, there is an overlap between the definitions of cyberexploitation and IW, and one could argue that cyberexploitation falls within the “range of...efforts that use information...against adversaries.” Cyberexploitation could thereby be the means to achieving IW ends. The full variety of capabilities, operations, and activities encompassed within the IW description are now encompassed under the umbrella term “operations in the information environment” (OIE). These types of OIE activities include, but are not limited to, key leader engagements, public affairs, civil-military operations, military information support operations, military deception, operations security, electromagnetic spectrum operations, space operations, and cyberspace operations.¹¹ These military actions affect drivers of behavior to inform, influence, and exploit target audiences while protecting friendly ones; however, adversarial state and non-state actors conduct their own version of OIE against their local populations, as well as against U.S. Armed Forces and their families.

⁹ Office of the Director of National Intelligence, *Intelligence Community Directive 204: National Intelligence Priorities Framework*, 2021, <https://www.dni.gov>; overall classification is UNCLASSIFIED.

¹⁰ Joint Chiefs of Staff, “Joint Publication (JP) 3-04, Information in Joint Operations,” 2022, III-25. https://jdeis.js.mil/jdeis/new_pubs/jp3_04.pdf.

¹¹ JP 3-04., B-7.

Conclusions

The IDA team found minimal written policy, strategy, instruction, or regulation within the DoD assigning specific responsibilities to prevent the cyberexploitation or online deception of members of the Armed Forces or their families. The IDA team was also unable to find any one source of empirical data that could support a conclusion that members of the Armed Forces and their family members are targeted at a higher rate in comparison with the general population. However, insights gained through the extensive interview process with representatives of 20 organizations across the Office of the Secretary of Defense, the Military Services, the Combatant Commands, the Joint Staff, federal agencies, academia, and industry indicate that this may be a growing area of concern for the Department.

It Is a “Seam” Issue. While cyberexploitation and online deception can be considered methods for enabling operations within the information domain, the methods are not typically executed through attacks on our networks, so it is not specifically a U.S. Cyber Command defensive responsibility. Much of the cyberexploitation and online deception activity are low-level scams aimed at stealing money from unsuspecting victims. Thus, this is also not a counterintelligence and insider threat mission.

The U.S. Military and Veteran Communities Are a Reflection of a Societal Issue. There is no meaningful way to opt out of commercial data collection, and this issue is not limited to the U.S. military and veteran communities, rather it represents a vulnerability for the whole of society. Everyday life requires each of us to partake in the services of online applications, shop online, use a smartphone, and connect with others through social media, making us vulnerable to having our personal data harvested, aggregated, curated and sold within the commercial data broker ecosystem. Government data at the federal, state and local levels, such as property records, driver license and driving records, voter registration records, and many other forms of government records are also available to be scraped or purchased. With the exception of a few states that have instantiated data privacy laws, there is no meaningful way to opt out of this data environment. The personal data about each of us is marketed and sold to companies who wish to sell us their products and services. Because of the volume of data that is collected, it is quite easy for commercial entities to target us with very personalized advertisements. In addition to companies who wish to engage us for legitimate commercial purposes, this same data is available to criminals who want to target us for more nefarious purposes like online scams or to foreign actors who wish to engage in disruptive information operations.¹² However, the demographics of the US Military and veteran populations make these communities an easy target for manipulation and exploitation. The negative effects of cyberexploitation and online deception can have negative impacts on readiness and can diminish unit cohesion, morale, and mission/combat effectiveness.

¹² Sherman, Justin, Haley Barton, Brady Klein, and Anushka Srinivasan. “Data Brokers and the Sale of Data on U.S. Military Personnel: Risks to Privacy, Safety, and National Security.” Duke University Sanford School of Public Policy. <https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/>.

Information Operations Are Enabled and Amplified Through Technology. The rapid expansion of AI technology, machine-manipulated data (and “deepfakes”) and commercially available information (CAI) domains (also known as “data brokers”) have expanded the ability to target individuals. In the not too distant past, it would have taken the resources of an adversarial nation state actor to do what someone now can do in a basement with very limited technical ability or computing resources. The CAI that is known and inferred about each of us is readily available for purchase and can be used for precise targeting of individuals or sub-populations for operations ranging from simple financial scams, to radicalization, to purposeful degrading of unit cohesion and morale, and for targeting individuals to commit espionage. The speed, scale, and capability of these technology and data tools are expanding exponentially, suggesting that the situation will get worse over time.

We Are Willing Consumers of the Enabling Technology. In most cases, we as consumers have enabled the data broker ecosystem by accepting the terms of service and end user license agreements (EULAs) for the social media and other commercial applications that we use on our smartphones and other Internet-enabled devices. Most consumers are unaware of the scope and magnitude of CAI that is available on each of us. The data that is used to target us for marketing, criminal activity, scams, extortion, disruption, radicalization, or espionage is not acquired illegally — it is typically purchased legally on the open market.

Balancing Security, Civil Liberties, Privacy, and Transparency. The risk to the DoD at the individual, unit, organization, or even sub-population level could be reduced by restricting individuals from using social media and similar apps on smartphones and disallowing them from participating in the digital marketplace. However, that would have a negative impact on the ability to attract and retain a highly qualified fighting force and would likely be challenged as imposing on an individual’s privacy, civil liberties, and freedom of speech.

Legislation, Regulation, and Policy Have Not Kept Pace with Technology. Legislative, regulatory, and policy solutions to cyberexploitation and online deception issues have not kept pace with the rapid expansion of the enabling technology and the adversary’s use of that technology to exploit our vulnerability to their advantage.

Proposed Recommendations to Congress

Enact a Data Privacy and Protection Act. Adopt and enact a data privacy framework within the United States analogous to the General Data Protection Regulation (GDPR) that has been in place within the European Union since 2016. There is currently no comprehensive federal data privacy law in the United States, but there have been ongoing discussions in Congress regarding the American Data Privacy and Protection Act (ADPPA).

The American Data Privacy and Protection Act, H.R. 8152, would create a comprehensive federal consumer privacy framework. The ADPPA regulation is similar to the GDPR in its coverage of entities and personal data.

From the Congressional Research Service:

The bill would prohibit covered entities from collecting, using, or transferring covered data beyond what is reasonably necessary and proportionate to provide a service requested by the individual, unless the collection, use, or disclosure would fall under one of seventeen permissible purposes. It also would create special protections for certain types of sensitive covered data, defined as sixteen different categories of data. Among other things, the bill would require covered entities to get a consumer's affirmative, express consent before transferring their sensitive covered data to a third party, unless a specific exception applies.¹³

The GDPR has been used as a model for the data privacy laws in Turkey, Mauritius, Chile, Japan, Brazil, South Korea, South Africa, Argentina, and Kenya. The UK retains the GDPR in identical form.

Enable a Meaningful and Comprehensive “Opt Out” Framework. Enact legislation that enables a meaningful “opt out” from the data broker ecosystem and allows members of the armed services and their families to “be digitally forgotten” by removing commercially available information from data broker database. Today there are limited means to opt out of the commercial data marketplace. And the methods that do exist are expensive, time-consuming, and are legally vague about whether the companies will actually adhere to the opt-out requests.

Proposed Recommendations to DoD

Expand Digital Persona Protection. Expand digital persona protection as detailed in DoDI O-2000.22 to include all DoD flag officers and senior executive personnel. The expanded DoDI O-2000.22 could also be supplemented by subsidizing a set of privacy enhancing services, tools and technologies to enable service members and families the opportunity to proactively manage their digital identity.

Assign Responsibility with Congruent Authorities. Establish a champion within the DoD to advocate for and enable the protection of digital identity management for members of the Armed Services and their families.

¹³ Congressional Research Service, Overview of the American Data Privacy & Protection Act, H.R.8152, Overview of the American Data Privacy and Protection Act, H.R. 8152 (congress.gov), August 31, 2022, p. 2.

Table of Contents

1.	Introduction	1-1
2.	Predatory Loans, Other Financial and Educational Products	2-1
	A. Types of Predatory Loans and Financial Products	2-2
	1. Payday Loans	2-3
	2. Car Title Loans	2-3
	3. Installment Loans	2-4
	B. Why Are Service Members Targeted?	2-4
	C. How Are Service Members Targeted?	2-5
	D. Educational Products and Deceptive Practices	2-6
	E. Impacts of Cyberexploitation and Deceptive Targeting of Service Members	2-7
	F. The Role of the Military Lending Act (MLA) on Predatory Lending	2-7
	G. Financial Literacy Education, Training, Programs, and Resources	2-9
3.	Unproven or Unnecessary Medical Treatments	3-1
	A. Social Media as a Threat Vector	3-3
	B. Multi-Level Marketing	3-5
4.	Ethnic and Racial Violent Extremism Messaging	4-1
	A. How Radicalization, Extremism, and Terrorism Are Defined	4-1
	B. Extremism and the Internet	4-6
	C. Risks and Vulnerabilities to Radicalization and Extremism	4-9
	1. Factors Associated with Radicalization	4-9
	2. Service Members and Radicalization	4-10
	3. Cyberexploitation by Extremist Groups and Foreign Maligned Actors	4-12
	D. Radicalization, Conspiracy Theories, and False Information	4-15
5.	Sextortion Case Studies	5-1
	A. Sextortion Definition and Relevance to the Department of Defense	5-1
	B. Cybercriminal Strategies	5-2
	1. Fake Child Pornography Strategy	5-2
	2. Fake Webcam Hacker Strategy	5-3
	3. Nude Photo Solicitation Strategy	5-4
	4. Demographic Vulnerabilities	5-5
	C. National Security	5-6
	D. Deepfake-enabled Sextortion	5-8
	1. The Evolution of Deepfaked Pornography	5-8
	2. Deepfaked Pornography Used for Online Sexual Harassment and Extortion	5-10
6.	The Role of Social Media in Cyberexploitation	6-1
	A. Navigating a “Post-Truth” World	6-1
	B. Social Media	6-2

C.	Machine-Manipulated Media (i.e., Deepfakes).....	6-5
7.	Intelligence Assessments.....	7-1
A.	Cyberexploitation Threats by Foreign Actors Relative to Other Forms of Information Warfare	7-1
B.	People’s Republic of China.....	7-2
C.	The Russian Federation	7-4
D.	Islamic Republic of Iran and Democratic People’s Republic of Korea (DPRK).....	7-6
E.	Islamic State of Iraq and al-Sham (ISIS).....	7-7
F.	Threat Overview	7-7
G.	How U.S. Intelligence Agencies Prioritize Cyberexploitation.....	7-8
H.	Office of the Director of National Intelligence (ODNI).....	7-9
I.	Defense Intelligence Agency (DIA).....	7-10
1.	Defense Intelligence Agency (DIA) Innovation Outreach Through NeedipeDIA.....	7-10
J.	National Security Agency	7-11
8.	DoD Education and Training.....	8-1
A.	DoD Actions to Reduce the Unauthorized Access of Personal Information for Malicious Purposes.....	8-1
B.	Military Service Actions to Reduce Cyberexploitation through Education....	8-1
C.	The DoD Cyber Crime Center (DC3)	8-2
D.	DoD Privacy, Civil Liberties, and Freedom of Information Directorate (DPCLD) Partnership with the National Counterintelligence and Security Center (NCSC)	8-3
9.	Conclusions and Recommendations.....	9-1
A.	Recommendations for Addressing Specific Avenues of Cyberexploitation ...	9-3
1.	Predatory Financial Practices	9-3
2.	Unproven and Unnecessary Medical Treatments.....	9-3
3.	Extremist and Racist Messaging	9-4
4.	Sextortion	9-5
5.	Cyberexploitation by Foreign Threats.....	9-6
B.	Overall Recommendations	9-6
	Appendix A. Interviewees	A-1
	Appendix B. References	B-1

Figures and Tables

Figure 3-1. Huberman’s Response to the Fabricated Video	3-5
Figure 3-2. Huberman’s Follow-up Response to the Fabricated Video	3-5
Figure 4-1. Categories of Extremist Ideologies	4-3
Figure 4-2. Meme Posted August 4, 2016, on the “Vietnam Veterans” Facebook Page.....	4-14
Figure 4-3. Fake Instagram Post Depicting a Mourning Family Member.....	4-15
Figure 6-1. Social Media Use by Active Military and the General Population.....	6-3
Figure 7-1. Beijing's Tactics for Global Media Influence	7-4
Figure 7-2. DIA NeedipeDIA Related to Cyberexploitation.....	7-11
Figure 7-3. NSA’s Best Practices for Securing Home Networks	7-11
Table 4-1. Protective and Risk Factors for Development of Radical Attitudes, Intentions, and Behaviors	4-10

1. Introduction

The Department of Defense's (DoD's) Deputy Chief Information Officer for Resources and Analysis tasked the Institute for Defense Analyses (IDA) to conduct a study on the cyberexploitation and risks of deceptive online targeting of members of the Armed Forces and their families. This task originated in section 589F of the 2021 National Defense Authorization Act (NDAA), which directed the Secretary of Defense to conduct the study and to provide a report to the Committees on Armed Services of the House of Representatives and the Senate.¹⁴

Per Section 589F of the 2021 NDAA,¹⁵ “‘cyberexploitation’ means the use of digital means and online platforms to knowingly access, or conspire to access, without authorization, an individual's personal information to be employed (or to be used) with malicious intent; or to deceive an individual with misinformation with malicious intent.”

The term *cyber exploitation* also appeared in 2016 California State Legislation and was defined as follows:

the non-consensual distribution of intimate photos and/or videos. The private material may have been obtained by ex-lovers, by ex-spouses, or by complete strangers through hacking, theft of a cell phone, during a computer repair, a false personal ad, or “photoshopping.” These photos or videos may be posted to humiliate and degrade the victims, to cause damage to their reputation, and/or used to extort them.¹⁶

The 2021 NDAA requested a report with the following information:

1. An assessment of predatory loans, other financial products, or educational products being targeted to members of the Armed Forces and their families. See Section 2 of this report.
2. An assessment of unproven or unnecessary medical treatments or procedures being targeted to members and their families. See Section 3.
3. An assessment of ethnic or racial violent extremism messages targeting member and their families. See Section 4.
4. A case-study analysis of three known occurrences of attempted cyber against members and their families. In addition to the cyberexploitation case studies described in Sections 2 through 4,

¹⁴ The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 116th Cong. Pub. L. 116-283, January 1, 2021.

¹⁵ Ibid.

¹⁶ <https://post.ca.gov/cyber-exploitation>.

the IDA team identified sextortion as a prevalent cyberexploitation problem. Section 5 defines sextortion and provides relevant case studies.

5. An assessment of the ways in which social media algorithms may amplify the targeting described in 1 through 3. See Section 6.

6. Intelligence assessments of the threats from foreign government and non-state actors carrying out the cyberexploitation of members and their families and creating or using machine-manipulated media. These assessments are combined in Section 7.

7. A description of action taken by the DoD to educate members and their families about actions that can be taken to reduce cyberexploitation threats. See Section 8.

8. Recommendations for policy changes to reduce the vulnerability of members of the Armed Forces and their families to cyberexploitation and deception, including recommendations for legislative or administrative action. See Section 9.

The IDA team performed an extensive literature search and conducted interviews with members of the department who represented various roles in the topical areas relevant to this engagement. The research team also conducted interviews with representatives of other government agencies, elements of the Intelligence Community (IC), research and development organizations, academia, industry, and other communities of interest.

2. Predatory Loans, Other Financial and Educational Products

The DoD defines *financial readiness* as “the state in which successful management of personal financial responsibilities supports a service member’s ability to perform their wartime responsibilities.”¹⁷ As such, “financial readiness is treated as a critical component of mission readiness.”¹⁸ Predatory lending¹⁹ as it relates to service members is not a new problem. In 2006, the DoD wrote a *Report on Predatory Lending Practices Directed at Members of the Armed Forces and their Dependents* in response to Section 579 of the National Defense Authorization Act for FY 2006.²⁰

DoD’s report takes a comprehensive look at the issue of predatory lending products that are targeted at service members and discusses strategies and practices to help reduce the impact and prevalence of predatory lending, with a particular focus on payday lending, one of the more ubiquitous predatory products at the time. The report cites a 2005 analysis by the Center of Responsible Lending, which estimated that “active-duty personnel are three times more likely than civilians to have taken out a payday loan. This report also estimates, again based on industry data, that one in five active-duty servicemembers were payday borrowers, and, finally, predatory payday lending costs military families over \$80 million in abusive fees every year.”²¹

DoD’s report offers six recommendations to protect service members against predatory lending:

1. Require that unambiguous and uniform price disclosures be given to all service members and family members with regard to any extension of credit (excluding mortgage lending).
2. Require a federal ceiling on the cost of credit to military borrowers, capping the annual percentage rate (APR) to prevent any lenders from imposing usurious rates.

¹⁷ Congressional Research Service R46983, *Military Families and Financial Readiness*.

¹⁸ Department of Defense, “2020 Status of Forces Survey,” *Annual Report on the Financial Literacy and Preparedness of Members of the Armed Forces*, 3.

¹⁹ Predatory lending occurs “when a lender uses unfair or deceptive tactics to lead a borrower into taking a loan that carries terms that benefit the lender at the borrower’s expense” (<https://www.nerdwallet.com/article/loans/personal-loans/what-is-predatory-lending>).

²⁰ National Defense Authorization Act for Fiscal Year 2006, 109th Cong. Pub. L. 109-163, 2006.

²¹ Department of Defense, *Report on Predatory Lending Practices Directed at Members of the Armed Forces and their Dependents*, April 9, 2006, 12.

3. Prohibit lenders from extending credit to service members and family members without due regard for the service member's ability to repay.
4. Prohibit provisions in loan contracts that require service members and family members to waive their rights to take legal action.
5. Prohibit contract clauses that require service members to waive any special legal protections afforded to them.
6. Prohibit states from discriminating against service members and family members stationed within their borders, and prohibit lenders from making loans to service members that violate consumer protections of the state in which their base is located.²²

A. Types of Predatory Loans and Financial Products

Typical exploitative characteristics of predatory lending include exorbitant interest rates (often in the triple digits) and excessive fees that are often undisclosed and/or hidden, as well as the frequent inclusion of contract provisions that require the borrower to waive their rights to take legal action against the lender. Other predatory characteristics include “loan flipping or repeat renewals that ensure profit without significantly paying down principal; loan packing with high cost ancillary products whose cost is not included in computing interest rates; loan structure or terms that transform these loans into the equivalent of highly secured transactions.”²³ The majority of predatory financial products tend to be short-term, with small loan amounts (around \$300-\$10,000) that are relatively quick and easy to obtain. Typically, the borrower must be 18 years old or older, complete a simple application, supply proof of income, and have a driver's license and bank account. These types of loans can be attractive to service members with lower incomes who may have bad credit, no credit, or no access to other types of credit. The loans are made regardless of the ability to pay.

It should be noted that, regardless of the type of loan, there are also regulations and laws that vary from state to state with regard to the interest rates that lenders are allowed to charge and the length of the loan, which can also affect the ability of these types of lenders to legally operate in a particular state. Some lenders intentionally operate in states with lax laws or little to no enforcement, so that the use of their predatory financial products can go unchecked. What is consistent across the array of financial products is the propensity of a service member to be negatively affected as a result of deceptive and predatory practices.

²² Ibid, 6–8.

²³ Ibid, 3.

1. Payday Loans

Payday loans are one of the most common type of predatory financial products targeted at service members. These are short-term loans, typically for small amounts, that include high interest rates and fees that are due in full on the borrower's next payday. This type of loan is secured by a borrower's personal check or an agreement in the loan contract to have the funds withdrawn electronically from the borrower's bank account. Payday loans come from a variety of sources, including storefront lenders, check cashing outlets, pawn shops, rent-to-own stores, and Internet sites.²⁴ Some of these lenders tend to exploit the opportunity of service members who may be dealing with an emergency situation, need to cover an essential expense, or simply need money to make ends meet. In fact, a 2013 Defense Manpower Data Center (DMDC) QuickCompass of Financial Issues survey question asked enlisted service members why they take out small-dollar loans. Of the respondents, 70% selected the option "to cover one or more unexpected essential expenses,"²⁵ and 31% said that they chose payday loans because they felt there was "no other alternative source for borrowing cash."²⁶ Payday lenders bet that service members will not be able to repay the amount in full on their next payday and will thus have to extend or rollover the loan by refinancing it, which incurs additional fees. Little or none of the refinanced amount is used to pay down the principal. Some borrowers even take out a loan from a different lender to pay off the original loan.

The global payday loan market, with a value of \$34.32 billion in 2022,²⁷ has only continued to proliferate over the past few decades. Payday lenders generate a tremendous amount of revenue for themselves, but affected service members often descend into a cycle of debt to avoid defaulting on their loan, which in turn detracts from their personal and professional life.

2. Car Title Loans

Car title loans are short-term, high-interest loans that are secured by the title to cars owned free and clear by the borrower. "The typical loan is for a fraction of the car's value, costs 300% APR, and has a one-month loan term. Title loans are often renewed month after month, without reduction in principal. Failure to repay can result in repossession of the vehicle. The high cost and risk of car title loans traps borrowers in repeated loan renewals in order to keep from losing essential transportation and key family assets."²⁸

²⁴ Ibid, 10.

²⁵ Department of Defense, *Report: Enhancement of Protections on Consumer Credit for Members of the Armed Forces and Their Dependents*, April 2014, 13.

²⁶ Ibid, 11.

²⁷ <https://www.vantagemarketresearch.com/industry-report/payday-loans-market-1512>.

²⁸ Department of Defense, *Report on Predatory Lending Practices Directed at Members of the Armed Forces and their Dependents*, April 9, 2006, 16.

3. Installment Loans

Installment loans are very similar to payday loans but are repaid in increments over a longer period of time, and the amounts borrowed can be much higher than those of payday loans. These types of loans can be used for cash, services like car repairs, or to purchase a broad range of retail items, such as electronics. Frequently, the interest and fees on these loans ultimately total more than the original price of the purchased items.

B. Why Are Service Members Targeted?

Service members have relative job security and a steady income that can be tapped by direct allotment, making it convenient for lenders to get their money. This population is comprised largely of young men and women who are away from home and receiving a pay check for the first time. According to the “2021 Demographics Profile of the Military Community,” 44.4% of active duty members are 25 years of age or younger.²⁹ They are prone to exploitation because they have lower salaries, may be inexperienced and not financially savvy enough to consider the consequences of getting “easy” money, or may not have the time to understand or even read the fine print of the predatory terms of a loan. During a 2013 hearing before the Committee on Commerce, Science, and Transportation, a senior naval civilian attorney attested that “...this sailor is my typical consumer client. They are young and the majority are junior in rank. Most have only a high school education. Their pay is guaranteed—recession proof, furlough proof, public knowledge, and easy to garnish. They have been removed from familiar surroundings and family support systems, and have been trained to respect and respond to authority—a critical mindset that is vital to the operation of the military.”³⁰

Also inherent in military culture is the expectation that service members should be prepared in all areas of their life. Financial readiness is particularly critical because the consequences of poor financial management, and the use of predatory financial products can be a detriment a service members’ ability to carry out his or her duties. Service members are expected to pay their financial obligations in a timely manner as prescribed by DoD Instruction (DoDI) 1344.09, *Indebtedness of Military Personnel*,³¹ and they can face a range of disciplinary actions if they do not. Many service members do not want to get in trouble or damage their careers, so, rather than report financial issues, they continue using and trying to pay off predatory financial products.

²⁹ Office of the Deputy Assistant of Defense for Military Community and Family Policy, *2021 Demographics: Profile of the Military Community*, 38.

³⁰ “Soldiers As Consumers: Predatory and Unfair Business Practices Harming the Military Community, Hearing before the Committee on Commerce, Science, and Transportation,” S. Hrg. 113-362, November 20, 2013, <https://www.govinfo.gov/content/pkg/CHRG-113shrg89464/html/CHRG-113shrg89464.htm>.

³¹ Office of the Under Secretary of Defense for Personnel and Readiness, DoD Instruction 1344.09, “Indebtedness of Military Personnel,” February 1, 2022, <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/134409p.pdf>.

Predatory lenders also exploit the circumstances that are common to service members, such as frequent relocations and deployments. Service members may not have time or be able to shop around for the best rates when they set up a household or move, and the use of predatory financial products is the easy, tempting route to cover some essential goods. In addition, when a service member is caught up in the burdensome cycle of debt, frequent moves and deployments can make it very difficult to negotiate with a predatory lender that is threatening to call your commander or to initiate a legal action against fraudulent or questionable debts.

C. How Are Service Members Targeted?

Shops offering payday loans and other predatory financial products proliferate outside military installations, making it easy for service members to access them when they need quick cash. The 2006 DoD report also noted that “military personnel stationed anywhere in the world can get high cost loans from lenders that advertise, accept applications, deliver and collect loans via the Internet. Military borrowers encounter a booming virtual market of small loan offers, payday loans, and ‘military’ loans via the Internet.”³² Seven years later, according to a 2013 QuickCompass Financial Issues survey, “enlisted Servicemembers obtained roughly half of their payday loans from storefronts (42%) and half from the internet (51%).”³³ Since these reports, payday and other predatory financial products have exploded online. Advertisements for predatory loans often surface on TikTok and Meta via video ads, even though TikTok and Meta have policies that are supposed to prohibit them. Instead, “many of the lenders that advertise on TikTok try to skirt regulations by creating new names for their service. By calling their interest rates a ‘tip’ or a ‘fee,’ lenders hope you won’t notice just how much interest you’ll actually pay.”³⁴ The predatory loan ads on social media platforms tend to target vulnerable populations, but data that is specific to targeting of service members is not evident.

Affinity marketing³⁵ is another common vector used to exploit service members at storefronts and online. Predatory lenders use service members’ patriotism to bait and target them. Predatory businesses targeting service members are often “draped in the American flag, many times they employ former servicemembers to heighten the trust of active duty soldiers, often times they hold themselves out as ‘specializing’ in serving the needs of soldiers or Federal employees. The business may have given money to a military support organization in order to receive a certificate

³² Department of Defense, *Report on Predatory Lending Practices Directed at Members of the Armed Forces and their Dependents*, August 9, 2006, 15.

³³ *Report: Enhancement of Protections on Consumer Credit for Members of the Armed Forces and Their Dependents*, April 2014, 21.

³⁴ *Ibid.*

³⁵ *Affinity marketing* is a direct marketing strategy in which a business partners with an organization or affinity group (a group of people with common interests) to “provide goods and services in exchange for a new market” (<https://www.techtarget.com/whatis/definition/affinity-marketing>).

or plaque of appreciation, which are then prominently displayed at a business location or website—again, capitalizing on common affinity marketing techniques.”³⁶ Predatory lenders have also used the official logos of government agencies or nonprofit organizations to promote and insinuate endorsement of their financial products.

D. Educational Products and Deceptive Practices

Many for-profit schools use affinity marketing, as well as aggressive recruiters or marketers, to target and exploit service members and veterans. Unfortunately, the quality of certifications, licenses, degrees, and training from these for-profit schools is lacking. Educational products from these schools are seen as less reputable and basically useless with respect to advancing a service member’s career. In some cases, students find out too late that the school was not properly accredited and that the credits they earned may not transfer to other institutions. Also, “for-profit colleges also tend to have a higher-than-average student loan default rate, which means that, in the end, the college experience there may hinder, rather than help, the careers and financial prospects of their graduates.”³⁷ Wasting time on educational products that provide no career benefit while potentially incurring student loan debt or putting benefits at risk can have a profoundly negative impact on service members.

Also troubling is that “for-profit schools have also used third party marketers in deceptive campaigns, going as far as to buy leads from marketers impersonating the military to lure consumers interested in serving our country to enroll in their schools.”³⁸ In 2018, the FTC charged Sunkey Publishing and Fanmail.com with running online ads encouraging military enlistment and using websites that masqueraded as legitimate military sites—domain names included army.com, armyenlist.com, and navyenlist.com—even though they had no affiliation with the military. The FTC alleged that the defendants sold this information to for-profit schools. The defendants’ sales representatives also bombarded consumers with calls and texts in which the representatives identified themselves as being from “Military Verification” and solicited interest in “military-friendly colleges.” The defendants also “allegedly used the email addresses they collected under the guise of military recruitment to advertise other products as well, like online dating, mortgages,

³⁶ “Soldiers As Consumers: Predatory and Unfair Business Practices Harming the Military Community, Hearing before the Committee on Commerce, Science, and Transportation,” November 20, 2013, <https://www.govinfo.gov/content/pkg/CHRG-113shrg89464/html/CHRG-113shrg89464.htm>

³⁷ <https://www.nytimes.com/2011/09/22/opinion/for-profit-colleges-vulnerable-gis.html>.

³⁸ Federal Trade Commission, “Prepared Statement of the Federal Trade Commission: Protecting Military Servicemembers and Veterans from Financial Scams and Fraud, Before the Committee on Oversight and Reform Subcommittee on National Security,” July 13, 2022, 6–7.

credit services, and scholarships.”³⁹ The case resulted in civil penalty judgements of \$11.1 million for Sunkey Publishing and \$1 million for Fanmail.com.⁴⁰

Service members are targeted in this manner primarily based on what is known as the 90/10 rule. Through the 1998 amendment to the Higher Education Act, Congress capped the percentage of revenue that for-profit schools can earn from the Department of Education programs at 90%, with the remaining 10% coming from non-federal sources. Currently, the GI Bill and military tuition assistance are counted as private, non-federal dollars, giving these schools a strong incentive to target and exploit service members and veterans. A provision in the 2021 American Rescue Plan closed this loophole, and the new regulations went into effect on January 1, 2023.⁴¹

E. Impacts of Cyberexploitation and Deceptive Targeting of Service Members

Predatory lending and predatory educational products can result in serious negative ramifications both for the service member and for his or her unit. A service member in poor financial health due to incurred debt from predatory loans may have their security clearance revoked or denied, and they may face criminal or non-judicial sanctions, which prevents them from deploying or participating in essential training and operations. This can reduce a unit's effectiveness, especially if there are a number of service members in the unit that cannot deploy. The low morale and pre-occupation with personal and financial difficulties can also distract the service member and affect job performance. Such distractions could have dangerous or potentially fatal consequences, depending on the job the affected service member performs. There may also be the potential for the service member to become compromised and sell classified information for money to get out of debt.

F. The Role of the Military Lending Act (MLA) on Predatory Lending

In 2006, Congress passed the Military Lending Act (MLA) in response to the six recommendations detailed in the 2006 *DoD Report on Predatory Lending Practices Directed at Members of the Armed Forces and their Dependents*. The MLA covers active duty service members, active National Guard or Reserve personnel, their spouses and certain dependents. The MLA was specifically “enacted to limit opportunities for active duty Servicemembers and their families to become involved with high cost products, which they often times continue to

³⁹ Ibid.

⁴⁰ Federal Trade Commission, “FTC Takes Action against the Operators of Copycat Military Websites,” September 6, 2018, <https://www.ftc.gov/news-events/news/press-releases/2018/09/ftc-takes-action-against-operators-copycat-military-websites>.

⁴¹ U.S. Department of Education, “90/10 – Questions and Answers,” <https://www2.ed.gov/policy/highered/reg/hearulemaking/2009/90-10-q-and-a.html>.

refinance.”⁴² The MLA established the Military Annual Percentage Rate (MAPR), which is a 36% interest cap on covered financial products. The MAPR calculation includes costs such as finance charges, credit insurance premiums and add-on credit-related products sold in connection with the credit, and fees such as application fees, participation fees, or fees for debt cancellation contracts (with some exceptions). It also includes no mandatory waivers of certain legal rights, no mandatory allotments, and no prepayment penalty.⁴³ However, MLA contained a narrow definition of consumer credit products and only covered a limited range of closed-end credit products, such as payday loans, auto title loans, and tax refund anticipation loans. As a result, predatory lending continued to persist as unprincipled predatory lenders found ways to circumvent the terms of the MLA.

Congress used the FY2013 NDAA to amend the MLA.⁴⁴ “The new rules apply to a broader range of closed-end credit products (e.g., fixed-term loans) and also extend regulations to open-end products (e.g., credit cards), thereby affecting a larger number of businesses. The new rules also include a safe-harbor provision for creditors to verify that an individual is a covered borrower through one or both of the following mechanisms: (1) the Defense Manpower Data Center (DMDC) MLA database, and/or (2) a report from a nationwide consumer reporting agency. The rules require lender compliance for consumer credit established on or after October 3, 2016, and for credit card accounts under an open-ended consumer credit plan on or after October 3, 2017.”⁴⁵ Loans that the MLA does not cover are “those with credit that is secured by the property being purchased and certain other secured loans. Generally, these loans include residential mortgages (any credit transaction secured by an interest in a dwelling), including financing to buy or build a home that is secured by the home, mortgage refinances, home equity loans or lines of credit, or reverse mortgages, a loan to buy a car when the credit is secured by the car and a loan to buy personal property when the credit is secured by the property.”⁴⁶ The amended MLA closed a number of loopholes, which drove some predatory lenders out of business, spurred some lenders to stop offering financial products to service members, and motivated other to modify their practices to comply with MLA regulations. Other lenders, however, continue to offer and promote predatory financial products.

⁴² *Report: Enhancement of Protections on Consumer Credit for Members of the Armed Forces and Their Dependents*, April 2014, 39.

⁴³ <https://www.consumerfinance.gov/consumer-tools/educator-tools/servicemembers/military-lending-act-mla/>

⁴⁴ The National Defense Authorization Act for Fiscal Year 2013, 112th Cong. Pub. L. 112-239, January 2, 2013.

⁴⁵ Congressional Research Service Report R46983, *Military Families and Financial Readiness*, January 12, 2022, 9.

⁴⁶ <https://www.consumerfinance.gov/consumer-tools/educator-tools/servicemembers/military-lending-act-mla/>

G. Financial Literacy Education, Training, Programs, and Resources

The DoD, along with a number of nonprofits, credit unions, partner organizations, and military advocacy groups, offers an abundance of resources, education, programs, and training to assist service members with making informed financial decisions during their military career. The Secretary of each Military Service is responsible for financial literacy training, and “DOD policy gives the Secretaries discretion on the method of delivery used for these trainings, and allows flexibility to include web- or computer-based training, instructor-led training, or structured self-development.”⁴⁷ Financial literacy training requirements were originally enacted by the FY2006 NDAA⁴⁸ and are outlined in Section 992 of Title 10 of the United States Code.⁴⁹ Amendments to financial literacy training requirements, which increased frequency and enhanced the content, were made in the FY2016 NDAA.⁵⁰ These amendments required DoD to “provide financial literacy training during ‘periodically recurring required training’”⁵¹ and at various touchpoints/significant life events in a service member’s career:

- During initial entry training.
- Upon arrival at first duty station and every subsequent duty station (for members in enlisted pay grades of E-4 or below and officers in the pay grade of O-3 or below).
- On the date of promotion of the member (for members in enlisted pay grades of E-5 or below and officers in the pay grade of O-4 or below).
- At each major life event during the member’s service, such as marriage, divorce, birth of a first child, or disabling sickness or condition.
- During leadership training.
- At transition points from a regular component to a reserve component and when separating or retiring from service.⁵²

The DoD also is required to provide certain financial counseling services to service members and their spouses, and “[t]he law requires installations with 2,000 or more servicemembers assigned to provide a full-time financial services counselor.”⁵³ Military Services are also required

⁴⁷ Congressional Research Service Report R46983, *Military Families and Financial Readiness*, January 12, 2022, 13.

⁴⁸ The National Defense Authorization Act for Fiscal Year 2006, 109th Cong. Pub. L. 109-163, January 6, 2006.

⁴⁹ Financial Literacy Training: Financial Services, 10 U.S.C. §992, (2023)..

⁵⁰ The National Defense Authorization Act for Fiscal Year 2016, 114th Cong. Pub. L. 114-92, November 25, 2015.

⁵¹ Congressional Research Service Report R46983, *Military Families and Financial Readiness*, January 12, 2022, 12.

⁵² *Ibid*, 12.

⁵³ *Ibid*, 13.

to offer one-on-one personal financial management counseling services, either “in-person at Military and Family Support Centers (MFSCs) located on the installations and, virtually, through the Military OneSource website.”⁵⁴ The DoD even offers a free app, SenSe, that provides service members, their families, and survivors with personalized financial education and tips.⁵⁵ The DoD Office of Financial Readiness website⁵⁶ provides information, resources, and tools to support financial management and readiness. Each February, DoD embarks on the Military Saves Campaign, sponsored by the Consumer Federation of America, which asks service members and their families “to pledge towards their own savings goals, and the campaigns are supported by banks and credit unions on military installations.”⁵⁷

Additional resources include MilSpouse Money Mission, a site whose mission is to “educate and empower military spouses to elevate their families by making smart money moves.”⁵⁸ Military Consumer, another site, is “a joint initiative to empower active duty and retired servicemembers, military families, veterans and civilians in the military community.”⁵⁹ Also, Military Consumer Month, which is recognized every July, provides a regular opportunity to bring financial issues to the forefront.

⁵⁴ Ibid, 14.

⁵⁵ <https://www.militaryonesource.mil/resources/mobile-apps/sense/>.

⁵⁶ <https://finred.usalearning.gov/>.

⁵⁷ *Report: Enhancement of Protections on Consumer Credit for Members of the Armed Forces and Their Dependents*, April 2014, 6–7.

⁵⁸ <https://www.milspousemoneymission.org/>.

⁵⁹ <https://www.militaryconsumer.gov/military-about-us>.

3. Unproven or Unnecessary Medical Treatments

The 2021 NDAA also requires “an assessment of unproven or unnecessary medical treatments or procedures being targeted to servicemembers and their families.”⁶⁰ It is difficult to determine whether a medical treatment or procedure is unproven or unnecessary, to include who has the responsibility and authority to categorize a treatment as proven or necessary. Questions of authority are compounded by social media, which is a primary vector for threats in this space.

Although service members and/or their families may be targeted for unproven or unnecessary medical treatments or procedures, it does not appear they are specifically targeted. Rather, it seems more likely that service members and their families, especially more junior personnel, are generally more active on social media and are thus subject to increased exposure to inaccurate and misleading medical information.

There is no single organization that defines medical treatments and procedures as proven/unproven or necessary/unnecessary. The Food and Drug Administration (FDA) evaluates foods, drugs, biologics, medical devices, electronic products that give off radiation, cosmetics, veterinary products, and tobacco products.⁶¹ According to the FDA, “health fraud drug products are articles of unproven effectiveness that claim to treat disease or improve health. In addition to wasting billions of consumers’ dollars each year, health scams can lead patients to delay proper treatment and cause serious—and even fatal—injuries.”⁶² The FDA views removal of its top priorities.⁶³

The 1994 Dietary Supplement Health and Education Act,⁶⁴ however, allows dietary supplements to bypass the FDA’s priority to restrict unnecessary and/or unproven medical products. The Act allows manufacturers to sell dietary supplements with unproven health claims and places the burden on the United States to prove a claim is false or misleading.⁶⁵ This allows tainted products to reach the market as dietary supplements. The FDA maintains on their website

⁶⁰ The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 116th Cong. Pub. L. 116-283, January 1, 2021. 2021 NDAA

⁶¹ <https://www.fda.gov/about-fda/fda-basics/what-does-fda-regulate>.

⁶² <https://www.fda.gov/drugs/buying-using-medicine-safely/medication-health-fraud>.

⁶³ <https://www.fda.gov/drugs/buying-using-medicine-safely/medication-health-fraud>.

⁶⁴ Dietary Supplement Health and Education Act of 1994, 103rd Cong. Pub. L. 103-417, 1994.

⁶⁵ <https://www.congress.gov/bill/103rd-congress/senate-bill/784>.

a list of tainted products in categories that include sexual enhancement, weight loss, body building, arthritis and pain, and sleep aids.⁶⁶

Medical procedures, however, are regulated by medical boards—not the FDA. The Federation of State Medical Boards (FSMB) oversees the 71 medical boards in the United States.⁶⁷ According to the FSMB, the District of Columbia and the U.S. territories have enacted laws and regulations that govern the practice of medicine and outline the responsibility of state medical boards to regulate that practice. This guidance is outlined in a state statute, usually called a Medical Practice Act.⁶⁸

The 10th Amendment of the United States Constitution allows states to regulate medicine.⁶⁹ As part of this responsibility, states license, discipline, and regulate health professionals.⁷⁰ The fact that there is no single national body to regulate health professionals and procedures can lead to discontinuities from state to state as new procedures arise.

Tricare, the predominate insurance provider for service members and their families, defines “medically necessary” as “appropriate, reasonable, and adequate for your condition.”⁷¹ Tricare does not cover “procedures that are unproven or experimental.”⁷² The Tricare website goes into further detail, stating that Tricare “excludes services and supplies that are not medically or psychologically necessary for the diagnosis or treatment of a covered illness (including mental disorder), injury, or for the diagnosis and treatment of pregnancy or well-child care. Additionally, all services and supplies (including inpatient institutional costs) related to a non-covered condition or treatment, or provided by an unauthorized provider, are excluded.”⁷³

A popular way to raise money for procedures that are not covered by insurance is through GoFundMe, a popular crowdfunding platform. GoFundMe even offers tips on how to run a successful medical fundraiser.⁷⁴ As of June 2023, the GoFundMe terms of service prohibit using the site to raise money for “drugs, narcotics, steroids, controlled substances pharmaceuticals or similar products or therapies that are either illegal, prohibited, or enjoined by an applicable

⁶⁶ <https://www.fda.gov/drugs/buying-using-medicine-safely/medication-health-fraud>.

⁶⁷ <https://www.fsmb.org/u.s.-medical-regulatory-trends-and-actions/guide-to-medical-regulation-in-the-united-states/introduction>.

⁶⁸ <https://www.fsmb.org/u.s.-medical-regulatory-trends-and-actions/guide-to-medical-regulation-in-the-united-states/introduction>.

⁶⁹ <https://www.fsmb.org/siteassets/education/pdf/best-module-text-intro-to-medical-regulation.pdf>.

⁷⁰ <https://www.fsmb.org/siteassets/education/pdf/best-module-text-intro-to-medical-regulation.pdf>.

⁷¹ <https://www.tricare.mil/CoveredServices/IsItCovered/Exclusions>.

⁷² <https://www.tricare.mil/CoveredServices/IsItCovered/UnprovenExperimentalProcedures>.

⁷³ <https://www.tricare.mil/CoveredServices/IsItCovered/Exclusions>.

⁷⁴ <https://www.gofundme.com/c/fundraising-tips/medical>.

regulatory body; legal substances that provide the same effect as an illegal drug; or other products, medical practices or any related equipment or paraphernalia that have been found by an applicable regulatory body to cause consumer harm.”⁷⁵ Using “active duty” as a search term and filtering for medical fundraisers returns a number of service members and/or related family members using GoFundMe to crowdfund medical procedures.

A. Social Media as a Threat Vector

Service members and their families rely on social media for connection, entertainment, and product recommendations, but this exposes them to misleading and potentially dangerous medial information. However, this is not unique to military members and their families. In 2022, PlushCare, a virtual primary care and mental health organization, conducted research to assess misinformation associated with mental health content on social media.⁷⁶ The organization analyzed 500 TikTok videos with the hashtags #mentalhealthadvice or #mentalhealthtips and labeled videos as misleading if any of the following three criteria were present:

- Is the advice inaccurate or potentially damaging?
- Is the host unqualified and does not provide a disclaimer?
- Do they encourage self-diagnosis?

The research team found that 83.7% of the mental health advice on TikTok is misleading based on these criteria and, while 54% of the advice contained accurate information, 31% of the videos contained inaccurate information.⁷⁷ Only 9% of the TikTokers dispensing medical advice had a relevant qualification.⁷⁸

“Scientese,” or scientific jargon, is also used to persuade the public. A 2004 study found that sales literature using the phrases “studies show” or “experts say” tended to convince people, even those with a science background, of the claim’s legitimacy.⁷⁹ Since this study’s release, it is likely that claims surrounding unproven products have grown more sophisticated and convincing.

Social media influencers, some of whom have massive reach and celebrity status, often use their platforms to dispense dubious lifestyle advice that can sway lifestyle decisions. In December 2022, Brian Johnson, known by the online persona “Liver King,” posted an apology video to his social media accounts where he admitted to using steroids—spending \$12,000 per month on

⁷⁵ <https://www.gofundme.com/c/terms>.

⁷⁶ <https://plushcare.com/blog/tiktok-mental-health/>.

⁷⁷ <https://plushcare.com/blog/tiktok-mental-health/>.

⁷⁸ <https://plushcare.com/blog/tiktok-mental-health/>.

⁷⁹ Jenifer Haard, Michael D. Slater, and Marilee Long, “Scientese and Ambiguous Citations in the Selling of Unproven Medical Treatments,” *Health Communication* 16, no. 4 (2004):, 411.

growth hormones—despite advocating eating raw meat and selling health supplements that he claimed to rely on to build and maintain his physique.⁸⁰ When he posted this video, he had 1.7 million Instagram followers, 4 million TikTok followers, and just under 250,000 YouTube subscribers.⁸¹ It is unknown how many service members were among his followers, but there is likely overlap between the young male adults he targeted and young male service members. Female service members and family members are targeted by influencers as well. In 2018, an influencer advertised Allergan breast implants and Botox at the same time that Allergan pulled its implants from European markets after a notice from the FDA.⁸²

Unproven and unnecessary medical treatments can go viral as well. In May 2023, apple cider gummies went viral on TikTok, with influencers claiming that the gummies helped with weight loss and bloating. Doctors questioning these claims, but people still purchased the gummies.⁸³ When confronted with a viral so-called miracle cure, social media users are often tempted to try these products without consulting their physician or registered dietitian.

Misleading medical advice is not limited to online influencers seeking reach and monetization. Even qualified medical experts are at risk of their likenesses being exploited to advocate for unnecessary and unproven medical procedures or treatments. In February 2023, a video advertisement appeared on TikTok and spread to other social media sites to promote a male libido product. The video, since removed on Twitter due to “a report by the copyright owner,” showed what appeared to be an interview discussing the benefits of this product between popular podcast host Joe Rogan and Dr. Andrew Huberman, a professor of neurobiology at Stanford Medicine who hosts his own popular podcast that shares peer-reviewed scientific study results and has more than one million Twitter followers.⁸⁴ The video is not so much a deepfake as a creative splicing of different portions of a real interview to give the impression Rogan and Huberman were endorsing the libido product, using Huberman’s prestige to garner a sense of legitimacy. Dr. Huberman responded to the video on Twitter (see Figure 3-1. and Figure 3-2.).

⁸⁰ https://www.youtube.com/watch?v=q_Vd7i4ZpgA.

⁸¹ <https://www.insider.com/liver-king-sued-customers-steroid-revelation-2022-12>.

⁸² <https://www.vox.com/the-goods/2019/2/15/18211007/medical-sponcon-instagram-influencer-pharmaceutical>.

⁸³ <https://www.newsweek.com/tiktok-apple-cider-vinegar-gummies-reduce-bloating-doctors-warning-1801477>.

⁸⁴ <https://twitter.com/JimmyFarley00/status/1624785773710151680?s=20>.

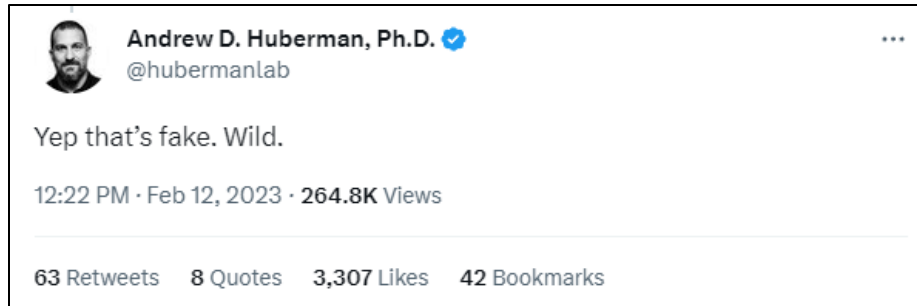


Figure 3-1. Huberman's Response to the Fabricated Video



Figure 3-2. Huberman's Follow-up Response to the Fabricated Video

This illustrates the challenges with fake celebrity endorsements and customer testimonials that will only grow more sophisticated with the state-of-the-art deepfake methodologies. Social media users, including service members and their families, need to view medical product endorsements with a critical eye.

B. Multi-Level Marketing

Service members and their family members are susceptible to direct selling or multi-level marketing (MLM) schemes involving health products. As service members and their families move from duty station to duty station, spouses tend to experience challenges with finding new employment. The comparatively lower pay for junior enlisted and junior officers also increases the likelihood of participating in these schemes to earn additional money. Common MLM products include jewelry, scented candles, and health products. The in-person communities common on military installations and among unit members can heighten the appeal of MLM schemes, and social media helps extend their reach.

Beach Body is one popular direct selling company. The product page for one of its health shakes claims that the shake is “meticulously crafted with powerful, nutrient-dense ingredients to

help you eat better, feel better and live better.”⁸⁵ However, there is a caveat in fine print at the bottom of the page: “These statements have not been evaluated by the Food and Drug Administration. This product is not intended to diagnose, treat, cure, or prevent any disease.”⁸⁶ Scientific evidence does not support Beach Body’s claims and suggests the shakes may even cause digestive issues.⁸⁷ But for military members and their spouses, Beach Body offers a program that waives the “coach business service fee” as a participation incentive⁸⁸ The catch, however, is that members must maintain a personal volume of at least 50 units of Beach Body product every 90 days to keep this waiver.⁸⁹ This personal volume includes products the member consumes themselves and any that they sell to others. Failing to meet this minimum results in permanent cancellation of the account, thereby compelling members to sell or absorb the units themselves. This not only encourages the use of meal replacement shakes with unevaluated health claims, it also results in financial loss for service members and their families.

TikTok banned MLM schemes in December 2020,⁹⁰ but this has not stopped MLM companies from skirting the ban. It Works, for example, started using TikTok to promote weight loss supplements promising quick results and financial gains for sellers in 2020.⁹¹ It also promoted its products on Facebook and Instagram.⁹² TikTok banned the main account for It Works in April 2022, but individual creators and influences have managed to avoid the ban and continue to promote It Works products on TikTok’s platform.⁹³

⁸⁵ <https://www.teambeachbody.com/shop/us/d/tropical-strawberry-plant-based-vegan-shakeology-SHKTropicalVegan>.

⁸⁶ <https://www.teambeachbody.com/shop/us/d/tropical-strawberry-plant-based-vegan-shakeology-SHKTropicalVegan>.

⁸⁷ <https://www.healthline.com/nutrition/shakeology-review#downsides>.

⁸⁸ https://faq.beachbody.com/app/answers/detail/a_id/2916/~military-waiver-program:-veteran,-reservist-&-active-duty.

⁸⁹ https://faq.beachbody.com/app/answers/detail/a_id/2916/~military-waiver-program:-veteran,-reservist-&-active-duty.

⁹⁰ <https://www.mediamatters.org/tiktok/predatory-mlm-scheme-thriving-tiktok>.

⁹¹ <https://www.mediamatters.org/tiktok/predatory-mlm-scheme-thriving-tiktok>.

⁹² <https://www.businessinsider.com/is-it-works-legit-2015-8>.

⁹³ <https://www.insider.com/tiktok-itworks-multi-level-marketing-diet-it-works-2022-4>.

4. Ethnic and Racial Violent Extremism Messaging

Neither Congress nor the executive branch of the federal government has an official definition for extremism. In fact, even the definition of extremism in the Oxford English Dictionary⁹⁴ requires individuals to insert their own perspectives. The thoughts, beliefs, and actions considered to be “extreme” are highly subjective and depend on a number of factors, including the nature of the political system, the prevailing political culture, a system of values, ideology, personal characteristics, experiences, and ethnocentrism.⁹⁵ Also, extremism and the myriad terms associated with it (e.g., terrorism, domestic terrorism, violent extremism, homegrown violent extremism, hate crime) have been used interchangeably by both the academic and operational (law enforcement and intelligence agencies) communities, with definitions changing depending on the context. The lack of a definition regarding extremism was a key theme explored during a 2019 conference held by the National Counterterrorism Center, which resulted in a finding for the need for a common set of terms and associated definitions that can apply across U.S. government agencies and departments with domestic terrorism investigative, intelligence, or prevention missions.⁹⁶

The IDA team examined research regarding the use of “ethnic or racial violent extremism messaging” as it relates to the cyberexploitation and online deception of service members and their families. In this section, we describe radicalization, extremism, and terrorism to contextualize the issue. We then describe the process of radicalization and how extremist organizations may use the Internet to exploit service members and their families. Finally, we discuss the extent of the issue and possible approaches to counter the cyberexploitation of service members by extremist organizations.

A. How Radicalization, Extremism, and Terrorism Are Defined

In general, radicalization is the cognitive and behavioral process of adopting to, changing, or strengthening a set of ideas that are considered extreme by society or the process by which

⁹⁴ The *Oxford English Dictionary* defines extremism as the “tendency to be extreme; disposition to go to extremes” <https://www.oed.com/view/Entry/67172?rskey=iXDkqO&result=1#eid>.

⁹⁵ Andrej Sotlar, “Some Problems with a Definition and Perception of Extremism within a Society,” In *Handbook of Policing in Central and Eastern Europe*, eds. Gorazd Meško Charles B. Fields, Branko Lobnikar, and Andrej Sotlar (New York: Springer, 2004), xx–xx..

⁹⁶ National Counterterrorism Center (NCTC), *Domestic Terrorism Conference Report*, Washington DC: NCTC, 2020.

individuals develop extremist ideologies, beliefs, and emotions (i.e., extremism), which can then serve as a motivation to engage in extremist actions or behaviors (e.g., an act of terrorism).⁹⁷ Radicalization does not necessitate that the radicalized individual engages in violent action—there are far more radicalized individuals in the world than there are individuals who will engage in an act of terrorism.⁹⁸ However, almost all individuals who engage in terrorist acts have gone through a radicalization process.⁹⁹

Extremism refers to ideologies, beliefs, and convictions that are considered to be on the fringes of the fundamental values of society and democracy—beliefs that often advocate the supremacy of a particular group (racial, religious, political, economic, social, etc.). Extremism can also refer to the methods (though not the specific acts) through which extremist actors try to achieve their aims.¹⁰⁰ Academic literature categorizes extremism into four main types based on the fundamental ideology or motivation for extremist actions and behaviors: left-wing, right-wing, single-issue, and politico-religious. The categories of extremist ideology are described in Figure 4-1, but some groups fit into multiple ideological categories. For example, the Aryan Nations could be considered both a right-wing and politico-religious extremist group because it was founded on the Christian identity and White supremacist movements.

⁹⁷ This process can take place over a period ranging from a few weeks to several years. See Jamie Bartlett, Jonathan Birdwell, and Michael King, *The Edge of Violence: A Radical Approach to Extremism*, 2010, and Borum, “Radicalization in Violent Extremism: violent extremism I: A Review of Social Science Theories,” *social science theories*, 2011.

⁹⁸ Roger Scruton, *The Palgrave Macmillan Dictionary of Political Thought*, 3rd edition, 2007; Peter R. Neumann, “The Trouble with Radicalization,” *Internal Affairs*, 89, no. 4 (2013): 873–893.

⁹⁹ Michael Wolfowicz, Yael Litmanovitz, David Weisburd, and Badi Hasisi, “Cognitive and Behavioral Radicalization: behavioral radicalization: A Systematic Review of the Putative Risk and Protective Factors,” *Campbell Systematic Reviews* 16 (2020): e1102.

¹⁰⁰ Kristen Klein & Arie Kruglanski, “Commitment and Extremism: A Goal Systemic Analysis,” *Journal of Social Issues* 69 no. 3 (2013): 419–435; Simona Trip et al., “Psychological Mechanisms in Radicalization and Extremism: A Rational Emotive Behavioral Conceptualization,” *Frontiers in Psychology* 10, no. 437 (2010): 1–8.

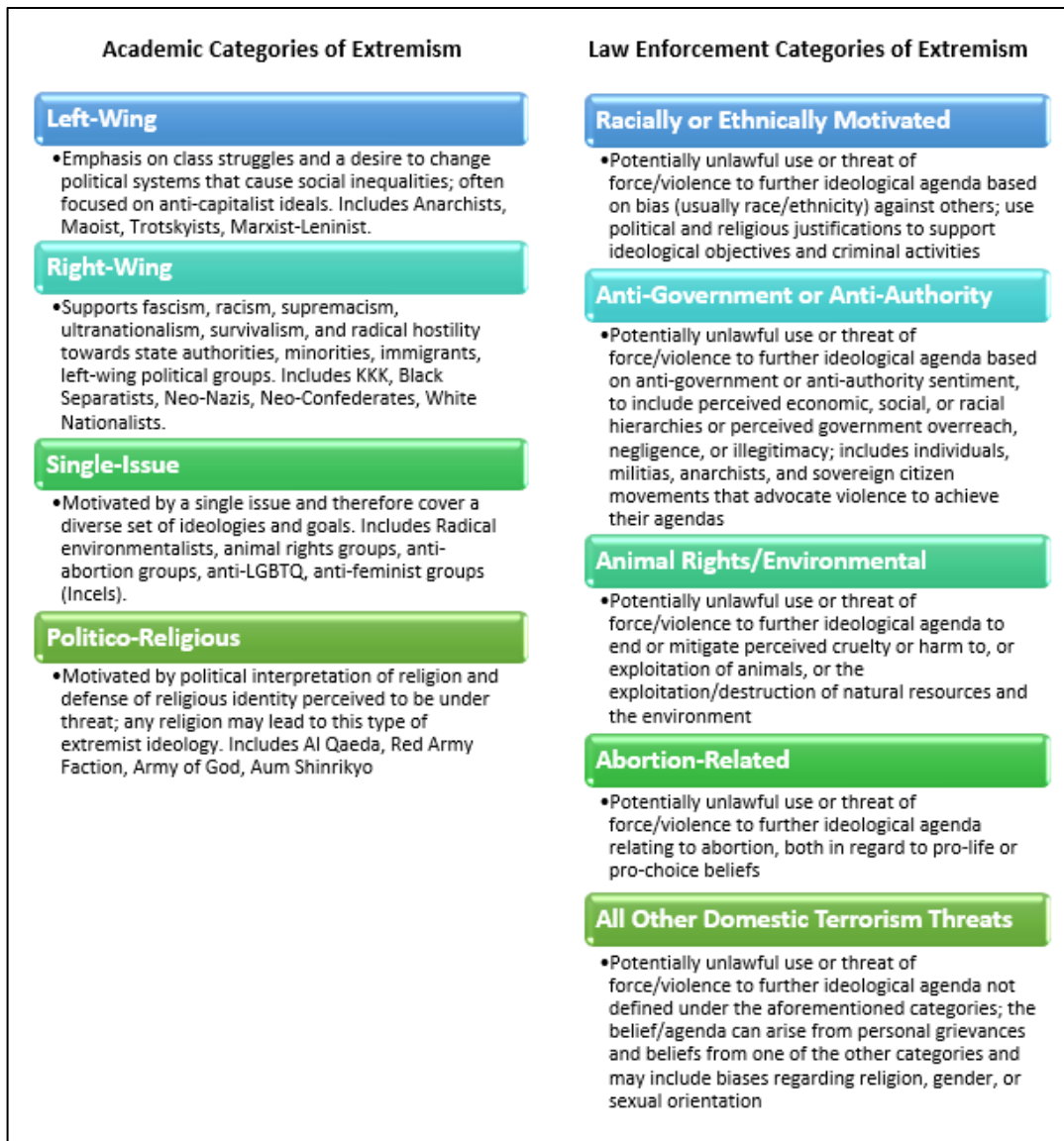


Figure 4-1. Categories of Extremist Ideologies

Law enforcement agencies categorize extremism differently than the academic literature. In 2020, the Federal Bureau of Investigations (FBI), U.S. Department of Homeland Security (DHS), and the Director of National Intelligence (DNI) jointly developed standardized definitions of terms relating to domestic terrorism and provided typologies of domestic terrorism threats. These groups use the term “violent extremism” because it is the aspect of violence, rather than the underlying extremist ideology or the advocacy of the ideology, that can be prohibited by law. Using this approach, law enforcement describes domestic threat typologies as racially or ethnically motivated extremism, anti-government or anti-authority extremism, animal rights or environmental extremism, abortion-related extremism, and other domestic terrorist threats. These categories are described in Figure 4-1. Similar to the academic community, law enforcement officials

acknowledge that extremist actor motivations vary and can arise from a blend of ideologies.¹⁰¹ The NDAA tasking focuses on what law enforcement categorizes as ethnically or racially motivated extremism; however, the cyberexploitation of service members and their families does not have to be limited to just one category (whether defined in academia or law enforcement).

The U.S. Government does not compile lists of groups affiliated with violent extremist ideology, because “advocacy of associated political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics may not constitute violent extremism, and may be constitutionally protected.”¹⁰² The FBI and other law enforcement agencies are allowed to obtain information regarding the activity and the role of an individual, group, or organization only as it relates to criminal activity and specifically to a federal crime that has been (or is about to be) committed. Thus, federal law enforcement agencies cannot investigate, collect, or maintain information on U.S. citizens to monitor extremist groups that advocate violent and non-violent action without the activity having a connection to criminal activity.¹⁰³

Given that federal law enforcement focuses first on the actions (which are criminal) and later examines the motivations, it is easy to see why there is such confusion regarding radicalization, extremism, and terrorism. While radicalization and extremism are the processes of internalizing an extreme ideology, terrorism is the action taken in support of the ideology. While extremism can be expressed through violent or non-violent action, terrorism, by definition, requires violence or the threat of violence. Although an individual can espouse violent extremist ideology without committing a crime, crossing the threshold of planning, preparation, and/or execution of a criminal act results in an act of terrorism.¹⁰⁴ Adding to the confusion, federal law enforcement uses the term “homegrown violent extremist (HVE)” to describe U.S. persons who are motivated by ideologies of foreign terrorist organizations. Both the FBI and DHS make a distinction between HVEs and domestic violent extremists, as the latter group supports the achievement of political or social goals using unlawful force or violence but is not directed or inspired by foreign terrorist goals.¹⁰⁵

Terrorism can be further classified as “domestic” or “international” as defined in Section 2331(5) of Title 18, United States Code. Per Section 2331(5), both categories of terrorism include violent acts or acts that are dangerous to human life that would be criminal law violations if committed in U.S. jurisdiction and include acts designed to intimidate or coerce civilian

¹⁰¹ Federal Bureau of Investigation and Department of Homeland Security, *Strategic Intelligence Assessment and Data on Domestic Terrorism*, 2021.

¹⁰² Ibid, 4.

¹⁰³ Ibid, 4.

¹⁰⁴ Gregory D. Miller, “Blurred Lines: The New ‘Domestic’ Terrorism,” *Perspectives on Terrorism* 13, no. 3 (2019): 63–75.

¹⁰⁵ Sacco, Lisa N. *Sifting Domestic Terrorism from Hate Crime and Homegrown Violent Extremism*. Congressional Research Service: Washington, DC, 2021.

populations, influence governmental policy through intimidation or coercion, or engage in mass destruction, assassination, or kidnapping as a means to affect governmental functions.¹⁰⁶ The difference is international terrorism acts take place primarily outside U.S. territorial jurisdiction or are considered transnational due to the manner in which the acts are accomplished, the persons the acts appear intended to intimidate or coerce, or the location where the perpetrator resides or operates from. The distinction is an important one because domestic terrorism is not, in itself, a criminal offense. Although the U.S. Code uses language from the 2001 Patriot Act to define “domestic terrorism,” it does not associate any criminal penalties with it, which means individuals cannot be charged with domestic terrorism at a federal level. At most, in cases of existing criminal convictions to cases that have been identified as “domestic terrorism,” federal prosecutors can request a terrorism enhancement that, if granted, can lengthen prison sentences.¹⁰⁷ Also, the distinction between international and domestic terrorism has been blurred by extremist organizations’ use of the Internet and social media to spread their ideologies and influence individuals on a global level. Although the federal government and academics have identified specific international extremist groups and organizations, the domestic extremist landscape is much more difficult to classify. Domestic groups often use decentralized networks or individual activity (e.g., lone actors) in lieu of centralized and/or hierarchical leadership. Additionally, the lack of clear leadership and access to a broad variety of extremist materials online leads to a lack of clear motivations on which to classify domestic extremist groups.¹⁰⁸

The extremist ideologies that serve as the basis for terroristic acts in the U.S. have shifted considerably over the past two decades. Post-September 11, 2001, extremist ideology was heavily inspired by al-Qaeda and the Islamic State, but it has changed to domestic extremism inspired by White supremacy, extremist militias, Christian nationalism, and similar ideologies. Extremist groups associated with these ideologies were responsible for two thirds of the terrorist plots and attacks in 2020.¹⁰⁹ In fact, Secretary of Homeland Security Alejandro N. Mayorkas issued a National Terrorism Advisory System (NTAS) Bulletin regarding the continued heightened threat environment across the United States on May 23, 2023. The NTAS Bulletin notes that “lone offenders and small groups motivated by a range of ideological beliefs and personal grievances continue to pose a persistent and lethal threat to the Homeland. Both domestic violent extremists (DVEs) and those associated with foreign terrorist organizations continue to attempt to motivate

¹⁰⁶ 18 U.S.C. § 2331(5).)

¹⁰⁷ Ware, Jacob & Ania Zolyniak, “Jan. 6 and Beyond: Why the U.S. Should Pass Domestic Terrorism Legislation,” *Lawfare* (May 28, 2023). <https://www.lawfareblog.com/jan-6-and-beyond-why-us-should-pass-domestic-terrorism-legislation>.

¹⁰⁸ Jones, Seth, Catrina Doxsee, Grace; Hwang, and Jared Thompson, “The Military, Police, and the Rise of Terrorism in the United States,” *CJIS Briefs* (April), Washington, DC.: Center for Strategic and International Studies, 2021.

¹⁰⁹ Ibid.

supporters to conduct attacks in the Homeland, including through violent extremist messaging and online calls for violence.”¹¹⁰

B. Extremism and the Internet

The use of the Internet to replicate and replace face-to-face interactions between extremist individuals and groups has been monitored by researchers and government agencies since the 1990s.¹¹¹ These assessments have shown how extremist organizations have used the benefits afforded by such technologies to decrease costs and improve efficiency, increase access to individuals on both the precipice of radicalization and those who are already adherents to the extremist ideology, and provide anonymity to individuals sharing extremist materials. In a 2018 report, Safer-Lichtenstein and his colleagues examined the use of social media by extremists in the United States. They found that in 2016 alone, social media played a role in the radicalization of almost 90% of those in the Profiles of Individual Radicalization in the United States (PRIUS) dataset.¹¹² When they expanded the data to the period of 2011 to 2016, they discovered that 73.2% of extremists in the dataset used social media to passively consume content, participate in communications with other extremists, and/or spread extremist propaganda. A majority of these individuals (76.9%) used social media as a means to supplement existing in-person relationships with fellow extremists and participate with closed, offline extremist networks. They also noted that social media has helped accelerate radicalization, citing an average of 18 months in 2005 compared with an average of 13 months in 2016.¹¹³

Evans and Williams (2020) classified extremist use of the Internet into five categories: financing, networking and coordination, recruitment and radicalization, inter- and intra-group knowledge transfer, and mobilization to action.¹¹⁴ Fundraising and financing activities that once occurred via print advertising and paper fliers are now done via websites, social media platforms, email distribution lists, messaging apps, and other virtual tools. Extremist groups use these

¹¹⁰ National Terrorism Advisory System Bulletin, “Summary of Terrorism-Related Threat to the United States,” 2023. <https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-may-24-2023>.

¹¹¹ S. M. Furnell and M. J. & Warren, “Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?” *Computers & Security* 18 no. 1 (1999): 28–34; Ian O. Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt, Michele Zanini, and Brian Michael Jenkins, *Countering the New Terrorism*, Santa Monica, CA: RAND Corporation, 1999. https://www.rand.org/pubs/monograph_reports/MR989.html.

¹¹² PIRUS is a database of 3,203 Islamist, far-left, far-right, and single-issue extremists who have radicalized to violent and non-violent extremism in the United States from 1948 through 2021. The PRIUS database was developed and is maintained by National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland, College Park. The database is freely available for download at <https://www.start.umd.edu/profiles-individual-radicalization-united-states-pirus-keshif>.

¹¹³ Aaron Safer-Lichtenstein, Gary LaFree, Michael Jensen, and Patrick & James, *Research Brief: The Use of Social Media by United States Extremists*. College Park, MD: START, 2018.

¹¹⁴ Alexandra T. Evans, and Heather J. Williams. *How Extremism Operates Online*, Santa Monica, CA: RAND Corporation, 2022.

Internet-based tools to publicize their financial needs directly to potential donors who can lend their support through traditional or online payment options, including crowdfunding websites and social media platforms with embedded donation applications.¹¹⁵ Although there is content monitoring on these traditional sites and apps, extremist groups have still managed to retain access. Some groups have moved to alternative platforms built specifically for extremist organizations, such as GoyFundMe, Hateon, and WeSearcher.¹¹⁶ Extremist organizations have also generated funds through merchandise sales directly through their own websites or existing online sales companies such as eBay, Amazon, and Etsy. Groups also sell self-published works through Amazon's CreateSpace and music-streaming services like Spotify or iTunes.¹¹⁷ These services have been particularly useful to extremist groups that are unable to meet in person or use a leaderless resistance strategy as a means to share tactical, operational, and ideological training widely, quickly, and with little cost to the group or the individual.¹¹⁸

Extremist organizations use social media and other online communication platforms to network within and among communities, socialize, and plan online and offline activities. Former extremists have described the utility of online discussion forums, chatrooms, and social media in successfully encouraging offline extremist-movement-related activities. One third of those interviewed reported having their first face-to-face interactions arranged through virtual interactions.¹¹⁹ Public and semipublic profiles of extremist organizations, their members, and their leadership allow not-yet-radicalized individuals easy access to extremist information and networks while giving existing members and leadership a means of identifying and vetting potential new members.¹²⁰

¹¹⁵ W. Chris Hale, "Extremism on the World Wide Web," *Criminal Justice Studies* 25, no. 4 (2012): 343–356.

¹¹⁶ Institute for Strategic Dialogue and the Global Disinformation Index. (2020). *Bankrolling Bigotry: An Overview of the Online Funding Strategies of American Hate Groups*. Institute for Strategic Dialogue: London. <https://www.isdglobal.org/isd-publications/bankrolling-bigotry/>; Tom Keatinge, Keen, Florence Keen, and Kayla Izenman, "Fundraising for Right-Wing Extremist Movements," *The RUSI Journal* 164, no. (2 (2019): 10–23.

¹¹⁷ Daniel Koehler, "The Radical Online: Individual Radicalization Processes and the Role of the Internet," *Journal for Deradicalization*, 1 (2014/2015): 116–134; Anti-Defamation League, *Funding Hate: How White Supremacists Raise Their Money*, New York: Anti-Defamation League, 2017. <https://www.adl.org/sites/default/files/adl-report-funding-hate-how-white-supremacists-raise-their-money.pdf>

¹¹⁸ Evans and Williams, How Extremism Operates Online; Hale "Extremism on the World Wide Web," 343–356.

¹¹⁹ Tiana Gaudette, Ryan Scrivens, and Vivek Venkatesh, . "The Role of the Internet in Facilitating Violent Extremism: Insights from Former Right-Wing Extremists," *Terrorism and Political Violence* 34, no. 7 (2022): 1339–1356.

¹²⁰ Laura Smith, "Lone Wolves Connected Online: A History of Modern White Supremacy," *New York Times*, 2021. Pete Simi, Steven Windisch, and Karyn Sporer, *Recruitment and Radicalization among U.S. Far Right Terrorists*, College Park, MD: START, 2016. https://www.start.umd.edu/pubs/START_RecruitmentRadicalizationAmongUSFarRightTerrorists_Nov2016.pdf

Evans and Williams (2020) also summarized three patterns regarding extremist groups and the Internet. First, although the extent of use varies, almost all extremist movements engage in some online activity, encouraged by the Internet's ability to support critical operations at lower costs, at a greater scale, and from any location. Second, extremist use of the Internet and Internet platforms parallels its use by non-extremists. As noted earlier, although Internet platforms prohibit or restrict their use for extremist purposes, extremist groups still use them far more than they do non-mainstream sites (i.e., an alternative Internet such as the deep web). Third, as mainstream platforms enforce restrictions and prohibitions on extremist materials, extremist groups will adapt to circumvent the restrictions through the use of counter-detection strategies and/or alt-tech platforms.^{121,122}

Extremist organizations use their members' skill sets to most effectively use the Internet in recruitment and radicalization. The Patriot Front,¹²³ for example, engages in "flash demonstrations," which are planned but do not have the required permits. Patriot Front embeds several camera operators within the demonstrations and collects images from members' body-worn cameras. Patriot Front's media team then edits these videos and circulates them on alt-tech platforms such as Gab and Telegram, while their social media team monitors online metrics such as number of mentions. This team also shares news coverage on private servers and identifies social media accounts for Patriot Front members to harass. The Patriot Front specifically designs their media packages to attract a younger audience and has been effective in galvanizing supporters to engage in actions on behalf of the organization. They portray members as "young warriors" who become elite warriors by focusing on fitness, diet, and participation in paramilitary drills prior to demonstrations.¹²⁴

The technological tactics used by extremist organizations to recruit and radicalize are not limited to traditional social media. Both Jihadist and right-wing extremists have modified mainstream games with images and messages that mirror their ideologies. These groups have even developed their own video games, where players can select avatars of known extremists and

¹²¹ Alexandra T. Evans, and Heather J. Williams. *How Extremism Operates Online*, Santa Monica, CA: RAND Corporation, 2022.

¹²² Alt-tech platforms provide alternatives to mainstream platforms such as Facebook and YouTube. These platforms have become popular with extremist groups because they eschew content moderation. See <https://knightcolumbia.org/blog/deplatforming-our-way-to-the-alt-tech-ecosystem> for more information.

¹²³ The Patriot Front, which split from Vanguard American in 2017, is a White supremacist group. Members maintain that their ancestors, who conquered America, bequeathed it to them, and the group therefore is only trying to preserve the ethnic and cultural origins of their members' White ancestors. The Anti-Defamation League states that the Patriot Front has been responsible for the majority of White supremacist propaganda distributed in the U.S. since 2019. Anti-Defamation League, (*Backgrounder: Patriot Front*, 2022.. <https://www.adl.org/resources/backgrounder/patriot-front>.

¹²⁴ MacKenzie Ryan, "A White Nationalists Pyramid Scheme: How Patriot Front Recruits Young Members". *The Guardian*, September 2, 2022.. <https://www.theguardian.com/us-news/2022/sep/02/patriot-front-recruits-members-young-pyramid-scheme>.

engage in game play that follows the extreme ideology such as killing individuals of different races or religions. Extremists have also livestreamed their attacks, posting video that mimics first-person shooter games and commentary that mimics gaming language. Brenton Tarrant's livestream of his attack on a Christchurch, New Zealand, mosque in 2019 was posted on Facebook and was viewed by at least 4,000 individuals. Facebook later removed another 1.5 million copies of the video. Because of the ease and efficiency of sharing the livestream of the attack, Tarrant's extremist views reached a large audience in a short amount of time and spurred copycat attacks against Muslims in other countries.¹²⁵ Extremist organizations track these situations that they deem as "successes," which not only solidifies their use of the Internet for recruitment and radicalization, but also highlights how the Internet serves as an efficient and effective tool for all extremist organizations.

C. Risks and Vulnerabilities to Radicalization and Extremism

1. Factors Associated with Radicalization

Radicalization is a dynamic multi-stage, multi-faceted cognitive and behavioral process that differs for each individual. Radicalization is influenced by a number of factors, and there is no single pathway or explanatory theory that can apply to all individuals or groups.¹²⁶ The process can be slow, taking place over a lifetime, or it can be quick, triggering immediate efforts to seek information on extremist groups and/or engage in extremist activities. However, Wolfowicz et al. (2020) identified individual-level factors associated with radical attitudes, intentions, and behaviors across five domains.¹²⁷ The contributing factors identified in the Wolfowicz study are summarized in Table 4-1.

¹²⁵ S. Bhatt and J. Mantua. "The Transnational Threat of Radicalization Through the Use of Online Gaming Platforms," In *Fostering Innovation in the Intelligence Community*, ed. C. Gruber (*Solutions to Combat a Dynamic Threat Environment*. Springer, in press). O. Brown "Right-Wing Extremism Online: Can We Use Digital Data to Measure Risk?" 2022. <https://crestresearch.ac.uk/comment/right-wing-extremism-online-can-we-use-digital-data-to-measure-risk/>.

¹²⁶ Borum, R. (2004). *Psychology of Terrorism*. Tampa, FL: University of South Florida. Borum, R. (2011). "Radicalization in Violent Extremism I: A Review of Social Science Theories," *Journal of Strategic Security* 4, no. 4: 7-36. doi:10.5038/1944-0472441.

¹²⁷ Wolfowicz, M., Y. Litmanovitz, D. Weisburd, and B. Hasisi, 2020, "Cognitive and Behavioral Radicalization: A Systematic Review of the Putative Risk and Protective Factors," *Campbell Systematic Reviews*, 16, e1102. doi:10.1002/cl2.1102.

Table 4-1. Protective and Risk Factors for Development of Radical Attitudes, Intentions, and Behaviors

	<i>Socio-demographic</i>	<i>Attitudinal</i>	<i>Experiential</i>	<i>Psychological / Personality</i>	<i>Criminological</i>
<i>Risk Factor</i>	Male gender	Radical attitudes	Prior incarceration	Anger	Criminal history
	Military experience	Personal injustice	Recent job loss	Authoritarian or fundamentalist	Deviant or radical peers
	Unemployment or welfare recipient	Low social integration	Online contact regarding extremist ideology	Mental health issues	Low self-control
	Relationship issues		Experienced violence		Thrill-seeking
	Immigrant		Abused		Radical family
	Religious convert		Bullied		
	Strict religious upbringing				
<i>Protective Factor</i>	Age	Law abidance			Attachment to school
	Parental involvement	Respect for law/government			
	Middle to high socio-economic status				
	Married				

Note. Adapted from Wolfowicz et al. (2020).

Although research can identify potential risk factors that may increase the likelihood of radicalization, each case must be examined to determine which characteristics and experiences served as drivers to radicalization for that individual and also to understand how the drivers interact with each other.

2. Service Members and Radicalization

There is no solid empirical evidence to support the idea that service members are more vulnerable to extremist radicalization than their civilian counterparts. There is some evidence that military training is linked to participation in terrorist violence among extreme Islamists, but similar linkage has not been demonstrated for other violent ideologies. Some studies suggest that previous participation in combat or military training experience could be a potential risk factor for

radicalization,¹²⁸ but other research suggests that military service can serve as a protective factor against criminal trajectories.¹²⁹ Finally, Extremism research often suffers from the problem of selection bias: most of the available data is on people who have radicalized. There is little to no available data that provides information on who is not radicalized.¹³⁰

A number of recently published reports, datasets, and a news alert from the Department of Justice provide additional examples of how service members and veterans have been involved with extremist plots and acts and the role of the Internet in these events. Though these reports identify how the individuals involved in these cases used the Internet, the reports do not examine the role the Internet played in recruitment. Cragin (2022) conducted case studies to understand how domestic extremist networks attempt to recruit members in the U.S. and determine if their recruitment attempts targeted at service members differed. The case studies represented both disrupted and successful violent extremist actions occurring between the Unite the Right rally in 2017 and the Capitol riots on January 6, 2021. Cragin found that each case involved current members of the National Guard or Army Reserves or veterans of the Army, Navy, Air Force, or Marine Corps. Facebook groups were the most common virtual recruitment tool, though other social media platforms (e.g., Discord chats, Telegram) provided outlets for discussion and recruitment as well. Recruitment patterns did not differ between civilian and military members: both were recruited online through social media and, in four of the five cases, offline at rallies as well. When recruitment events took place at political rallies and protests, it seemed that veterans actively sought out other veterans for recruitment.

The Department of Justice released a press briefing on March 3, 2023, regarding Ethan Phelan Melzer, who was active-duty Army when he was captured for attempted murder of U.S. service members, providing and attempting to provide material support to terrorists, and illegally transmitting national defense information. Meltzer pled guilty to not only planning a jihadist attack on his Army unit, but also sharing sensitive details about the unit to members of a number of extremist organizations, including the Order of the Nine Angels (a White supremacist, neo-Nazi, pro-jihadist group). He subscribed to a number of encrypted online forums where he consumed extremist propaganda and watched videos of jihadist attacks on U.S. troops and facilities, videos

¹²⁸ Per Dzhekova et al. (2017) and Smith (2018).

¹²⁹ M. Hafez, “Radicalization in the Persian Gulf: Assessing the Potential of Islamist Militancy in Saudi Arabia and Yemen,” *Dynamics of Asymmetric Conflict* 1 (2008): 6–24.

¹³⁰ J. Dawson (2023). “Who Controls the Code, Controls the System: Algorithmically Amplified Bullshit, Social Inequality, and the Ubiquitous Surveillance of Everyday Life.” *Sociological Forum*, n/a(n/a). <https://doi.org/10.1111/socf.12907>.

showing executions of civilians and soldiers, and other far-right, neo-Nazi materials. Meltzer received a 45-year prison sentence for his crimes.¹³¹

3. Cyberexploitation by Extremist Groups and Foreign Maligned Actors

Although there is currently no open-source evidence available showing that extremist organizations use deepfakes for recruitment and radicalization of service members and their families, a two-year investigation by the Vietnam Veterans of America (VVA) found “persistent, pervasive, and coordinated online targeting of American servicemembers, veterans, and their families by foreign entities who seek to disrupt American democracy”.¹³² These foreign maligned actors’ efforts closely resemble those of extremist organizations, though their motivations differ. Foreign actors engaging in cyberexploitation primarily seek to exacerbate existing political discord. For example, the Russian Internet Research Agency (IRA) targeted followers of congressionally chartered veterans service organizations with political ads during and after the 2016 U.S. Presidential election to widen divisions between Americans at differing ends of the political spectrum. But attempts to create discord among U.S. citizens, including service members, veterans, and their families, is not limited to just Russia. Facebook’s country of origin tool, which identifies the administrators of pages with more than 110,000 followers and people who have purchased political ads, shows that known Russian propaganda and politically divisive messaging has been spread by individuals in more than 80 foreign countries (mostly Eastern Europe and Vietnam).

Foreign actors also administer fake Facebook pages to perpetrate financial fraud and spread anti-American propaganda.¹³³ Gallacher et al. (2017) reported that service members and veterans are targets for foreign adversaries because individuals in both groups are often politically engaged to the degree that they regularly vote and/or serve in public office. Up to one third of the federal workforce is comprised of veterans due to their preferred status in federal hiring.¹³⁴

Foreign Facebook page administrators create fake veteran and military accounts claiming to be a veteran who works for a reputable veterans’ organization. They send friend requests to veterans’ advocates to connect with people who shape federal policy. These fake accounts are used

¹³¹ Department of Justice, *Justice News: Former U.S. Army Soldier Sentenced to 45 Years in Prison for Attempting for Murder Fellow Servicemembers in Deadly Ambush*, March 3, 2023. <https://www.justice.gov/opa/pr/former-us-army-soldier-sentenced-45-years-prison-attempting-murder-fellow-service-members>

¹³² Kristofer Goldsmith. (2019). *An Investigation into Foreign Entities Who Are Targeting Servicemembers and Veterans Online*. Vietnam Veterans of American, p. 6. <https://vva.org/wp-content/uploads/2019/09/VVA-Investigation.pdf>

¹³³ Ibid.

¹³⁴ John D. Gallacher, Vlad Barash, Philip N. Howard, and John Kelly, “Junk News on Military Affairs and National Security: Social Media Disinformation Campaigns Against US Military Personnel and Veterans,” *Data Memo 2017.9*, Oxford, UK: Project on Computational Propaganda, 2017. <http://comprop.oii.ox.ac.uk/research/working-papers/vetops/>.

to infiltrate public and private Facebook pages and groups to spread propaganda and false news and gather information on the followers' military experiences. For example, the "American Veterans of Vietnam" closed Facebook group is administered by individuals in Russia, Ukraine, and Italy and solicits military experience information by posting images of military equipment and asking followers to respond if they have used the weapon. Such groups also seek out the assistance of fellow veterans (unsuspecting of the fraudulent nature of the group) to serve as moderators of the sites to "keep the group free of spammers." In doing so, real veterans inadvertently provide another illusion of legitimacy to such groups.¹³⁵

Goldsmith (2019) reported that fake Facebook (and Twitter, Instagram, etc.) accounts often use the real VVA logo and registered trademark to give the illusion of legitimacy. These pages post positive memes that evoke feelings of camaraderie, social connection, and celebration to build an audience. But they also post deceptive or manipulated news stories and political content with the goal of inciting anger from the page's followers. These posts target two groups: those who agree with the content and will share it, spreading the message more broadly, and those who so strongly reject the message that they respond both to the page and to others who have posted comments in support, thus successfully creating conflict and deepening divisions. The posts often include emoticons that encourage supporters to respond with a heart or angry face reaction. These reactions are then identified by Facebook's algorithm as being associated with individuals more invested in the content than a follower who responded with a thumbs up (or "like") response. This drives the algorithm to provide users with similar content, creating echo chambers that simulate the feeling of a community of people with similar views. For example, Figure 4-2 (adapted from Figure 34 in the Goldsmith report) shows a meme posted by "Vietnam Veterans," a fake Facebook page administered from Bulgaria. On the day of the post (August 4, 2016), it had already been shared 342 times. The admins included a heart in their post to encourage supporters to respond in kind, which would enable the Facebook algorithm to identify them as targets for additional material. The followers who responded with "likes" and/or comments self-identified as individuals who are affected by such political content.

¹³⁵ Kristofer Goldsmith. (2019). *An Investigation into Foreign Entities Who Are Targeting Servicemembers and Veterans Online. Vietnam Veterans of American*. <https://vva.org/wp-content/uploads/2019/09/VVA-Investigation.pdf>.

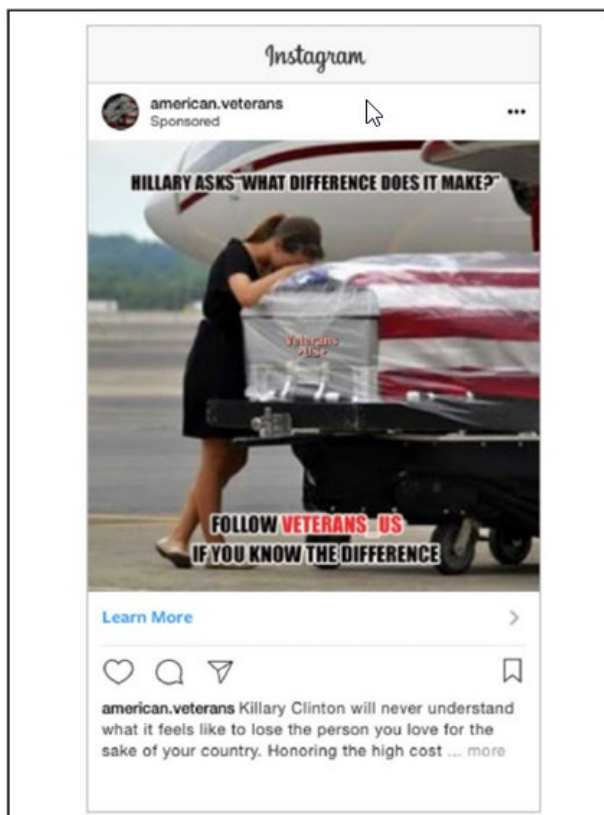


Note. Adapted from Figure 34 in Goldsmith report. This Facebook page is administered from Bulgaria and is not associated with the VVA.

Figure 4-2. Meme Posted August 4, 2016, on the “Vietnam Veterans” Facebook Page

In addition to the racist and/or xenophobic memes used to generate attention, these admins also use actual, publicly available photographs of current and former service members and other important individuals in history. They also exploit families in mourning by politicizing photographs taken at the gravesites of fallen service members, as shown in Figure 4-3. Other divisive posts include images with text made to appear as if President Obama was disrespectful toward veterans while President Trump was not, memes referencing Colin Kaepernick’s kneeling-for-the-anthem campaign juxtaposed against an image of a service member’s casket (with text stating that supporters of the campaign are unpatriotic, a theme that exacerbates the political divide), holidays such as Memorial Day, images of women in the military with text highlighting their gender, and elderly veterans seeking former military colleagues or asking for likes or responses indicating respect.¹³⁶

¹³⁶ Ibid.



Note. Adapted from Figure 134 in Goldsmith. Notice that the text instructs supporters to follow the poster.

Figure 4-3. Fake Instagram Post Depicting a Mourning Family Member

D. Radicalization, Conspiracy Theories, and False Information

There is no clear and direct pathway to radicalization. Each individual with extremist beliefs became radicalized in their own way and in their own time. Likewise, not all radicalization occurs through recruitment by an extremist organization. Some aggrieved individuals self-radicalize and seek out extremist materials and organizations on their own.¹³⁷ The ubiquity of social media poses a particular risk for DoD, because it not only exposes service members to influences from outside the bubble of the military environment, it may also make it more difficult for leaders and peers to detect the presence of maligned influences. The ubiquitous sharing of goals, tactics, and rhetoric on message boards and through informal online networking allows multiple groups to adopt similar extremist orientations.¹³⁸ Often times, the viral spread of information goes hand-in-hand with the production of information cascades in which users share information without fully understanding

¹³⁷ R. Bradbury, T. Bossomaier, and D. Kernot, "Predicting the Emergence of Self-Radicalizations through Social Media: A Complex Systems Approach," in *Terrorists' Use of the Internet*, eds. M. Conway, L. Jarvis, O. Lehané, S. Macdonald, and L. Nouri (IOS Press, 2017): 379–389.

¹³⁸ A. Perliger, "Deciphering the Second Wave of the American Militia Movement," *CARR Policy Insight*, Center for Analysis of the Radical Right, January 2021.

or knowing (or caring) about the accuracy of that information. The proliferation of such misinformation and disinformation make the Internet a potent breeding ground for extremist radicalization.¹³⁹

Some extremist groups and foreign maligned actors intentionally spread misinformation and disinformation to propagate dissent and build support for their radical agendas. This strategy may take the form of endorsing or spreading conspiracy theories.¹⁴⁰ Some conspiracy theories seek to attack or discredit specific individuals or groups, such as minorities. Because conspiracy theories are associated with an overall distrust of mainstream narratives and governing institutions, they also play a role in the development and spread of anti-government ideologies. In addition, conspiracy theories that condone the use of violence as a means to rectify perceived grievances may normalize terrorism, helping to move individuals from radicalization to terrorism.¹⁴¹ One review of the literature, ideology, and propaganda of more than 50 extremist groups in Europe and the United States determined that extremist groups use conspiracy theories to increase threat perception and in-group identification, which exacerbates “us” versus “them” rhetoric, increases group polarization and group think, and intensifies extremist beliefs.¹⁴²

The starting point to radicalization often includes a real or perceived event that serves as a point of grievance and justification for hateful actions, and conspiracy theories can enable this process. Conspiracy theories work, in part, because people are susceptible to the truth-by-repetition effect, even in regard to highly improbable statements. Due to processing fluency, repetition makes it easier to cognitively process information, which is misinterpreted as a signal that the information

¹³⁹ For a comprehensive review of the psychology (accepting, sharing, and correcting false information), see Greifeneder et al. (2021) and Ecker et al. (2022). Although both mis- and disinformation involve the sharing of false information, the motivation behind the sharing differs between the two. In misinformation, false information is shared without malicious intent (e.g., the sharer either believes the information to be true or has not vetted the information for accuracy). In disinformation, the sharer is aware that the information is false and shares it with malicious intent. J. Jerit, and Y. Zhao, “Political Misinformation,” *Annual Review of Political Science* 23 (2020): 77–94.

¹⁴⁰ A conspiracy theory generally alleges the existence of secret plots by multiple actors who are working to seize political or economic power, violate rights, infringe upon established agreements (e.g., the Constitution), withhold critical secrets or information, or alter foundational institutions. Although a conspiracy theory may reference some actual facts and/or events, it generally relies upon questionable connections and linkages that may or may not be true. A. Levinsson, C. Miconi, Z. Li, R. L. Frounfelker, and C. Rousseau, “Conspiracy Theories, Psychological Distress, and Sympathy for Violent Radicalization in Young Adults during the COVID-19 Pandemic: A Cross-Sectional Study,” *International Journal of Environmental Research and Public Health* 18 (2021): 7846–7858. doi:10.3390/ijerph18157846; K. M. Douglas, J. E. Uscinski, R. M. Sutton, A. Cichocka, T. Nefes, C. S. Ang, and F. Deravi, “Understanding Conspiracy Theories,” *Political Psychology* 40, Suppl. 1 (2019): 1–33. doi:10.1111/pops.12568

¹⁴¹ G. J. Rousis, F. D. Richard, and D.-Y. D. & Wang, “The Truth Is Out There: The Prevalence of Conspiracy Theory Use By Radical Extremist Organizations,” *Terrorism and Political Violence* (2020): 1–19. doi:10.1080/09546553.2020.1835654

¹⁴² J. Bartlett, and C. Miller, *The Power of Unreason: Conspiracy Theories, Extremism and Counterterrorism*, London: Demos, 2010.

is true.¹⁴³ Recent research indicates that conspiracy mentality is associated with stronger intentions to engage in extremist violence.¹⁴⁴

Although conspiracy theories are not necessarily classified as “extremist,” they have contributed to radicalization and incitement of criminal acts and violence. The U.S. Secret Service’s National Threat Assessment Center published a report on mass attacks on the public from 2016 to 2020. Although some type of personal grievance was the primary motive for most attacks, one quarter of the 173 mass attacks during this four-year window were motivated by conspiracy theories or hateful ideologies. Six of the individuals motivated in this way were radicalized online.¹⁴⁵

There are an endless number of conspiracy theories that can be used to cyberexploit individuals, but QAnon is unique due to both its prominence in the U.S.¹⁴⁶ and its connection to the U.S. military. Although QAnon first appeared online on 4chan in October 2017, it was associated with the 2016 Pizzagate conspiracy theory¹⁴⁷ that led Edgar M. Welch to travel on December 4, 2016, from North Carolina to Washington, D.C.’s Comet Ping Pong pizzeria with a handgun and assault-style rifle to free children he believed were trapped in the restaurant’s basement as part of a sex-trafficking ring. After storming the restaurant with his weapons and finding no children and no basement, he surrendered to police, was charged with federal and local weapons violations, and sentenced to four years in prison (with additional time under supervised release). Although he says he regrets his actions, Welch still maintains that elements of the Pizzagate theory are true.¹⁴⁸

¹⁴³ D. Lacassagne, J. Béna, and O. Corneille, “Is Earth a Perfect Square? Repetition Increases the Perceived Truth Of Highly Implausible Statements,” *Cognition* 223 (2022): 105052.

¹⁴⁴ B. Rottweiler, and P. Gill, “Conspiracy Beliefs and Violent Extremist Intentions: The Contingent Effects of Self-Efficacy, Self-Control, and Law-Related Morality,” *Terrorism and Political Violence* 34, no. 7 (2020): 1–20.

¹⁴⁵ National Threat Assessment Center. (2023). *Mass Attacks in Public Spaces: 2016-2020*. U.S. Secret Service, Department of Homeland Security.

¹⁴⁶ Per a 2021 poll by the Public Religion Research Institute, 16 percent of Americans believed in QAnon. Public Religion Research Institute, *The Persistence of QAnon in the Post-Trump Era: An Analysis of Who Believes in the Conspiracies*, 2022. <https://www.prrri.org/research/the-persistence-of-qanon-in-the-post-trump-era-an-analysis-of-who-believes-the-conspiracies/>

¹⁴⁷ The Pizzagate conspiracy theory states that emails from John Podesta (chair of Hillary Clinton’s 2016 Presidential bid) contained coded words and satanic symbols indicating a secret child sex-trafficking ring at Comet Ping Pong; Cecilia Kang, “Fake News Onslaught Targets Pizzeria as Nest of Child-Trafficking,” *The New York Times*, November 21, 2016. <https://www.nytimes.com/2016/11/21/technology/fact-check-this-pizzeria-is-not-a-child-trafficking-site.html>.

¹⁴⁸ Fruzsina Eordogh, “With Pizzagate, Is Cybersteria The New Normal?” *Forbes*, December 7, 2016. <https://www.forbes.com/sites/fruzsinaeordogh/2016/12/07/with-pizzagate-is-cybersteria-the-new-normal/?sh=3930d5e62b68>; “North Carolina Man Pleads Guilty to Charges in Armed Assault at Northwest Washington Pizza Restaurant,” United States Attorney’s Office, District of Columbia, March 24, 2017; “North Carolina Man Sentenced to Four-Year Prison Term For Armed Assault at Northwest Washington Pizza Restaurant,” United States Attorney’s Office, District of Columbia, June 22, 2017; Amarnath Amarasingam, and

The actual origins of QAnon are unknown; however, it is based on an amalgamation of far-right conspiracy theories that claim that former President Donald Trump is secretly planning a war against an elite clique of satanic pedophiles (comprised of Democratic politicians and Hollywood celebrities) who have corrupted every level of government.¹⁴⁹ Because QAnon followers are encouraged to conduct their own research into areas that they feel are corrupt, they play an active role in the movement's narratives. This directive has led to an expansion of QAnon's original conspiracy theory to a degree that greatly complicates the ability to counter such narratives. QAnon's conspiratorial claims have broadened to include an extreme view on government corruption and false elections, but militant and anti-establishment ideology remains at its core. These beliefs resonate with other domestic far-right extremist movements, including militias, anti-government groups, White nationalists, and neo-Nazi extremist groups.¹⁵⁰ QAnon supporters have run for and gained prominent seats in public office.¹⁵¹ QAnon has also influenced some former service members to propagate its message and even take action. Of the 34 QAnon followers arrested for the Capitol insurrection, 12 had previously served in the military.¹⁵² Because of the increased reporting of crimes committed in support of QAnon, some national security experts have identified it as an emerging danger that could become on par with other, more traditional extremist threats, and the FBI has issued warnings that some QAnon followers may target liberal political figures and others deemed to be enemies of QAnon with deadly force.¹⁵³

Human Rights First reported that QAnon's focus on the U.S. military is central to its ideology, which makes it different from other extremist movements and conspiracy theories. The most

Marc-André Argentino, "The QAnon Conspiracy Theory: A Security Threat in the Making?" *CTC Sentinel* 13, no. 7 (2020): 37–44.

¹⁴⁹ M. Rothschild, *The Storm Is Upon Us: How QAnon Became a Movement, Cult, and Conspiracy Theory of Everything*, Melville House, 2021.

¹⁵⁰ Amarnath Amarasingam, "The Impact of Conspiracy Theories and How to Counter Them: Reviewing the Literature on Conspiracy Theories and Radicalization to Violence," in *Jihadist Terror: New Threats, New Responses*, eds.. In Anthony Richards, Devorah Margolin, and Nicolo Scremin (London: IB Taurus, 2019), 27–40.).

¹⁵¹ Jack Brewster. "Congress Will Get Its Second QAnon Supporter, as Boebert Wins Colorado House Seat,," *Forbes*, November 4, 2020. <https://www.forbes.com/sites/jackbrewster/2020/11/04/congress-will-get-its-second-qanon-supporter-as-boebert-wins-colorado-house-seat/?sh=348a5ef6568f>

¹⁵² Michael Jensen and Sheehan Kane, *Research Brief: QAnon Offenders in the United States* (College Park, MD: National Consortium for the Study of Terrorism and Response to Terrorism, 2021); Human Rights First, "Digital Soldiers": *QAnon Extremists Exploit U.S. Military, Threaten Democracy* (Washington, DC: Human Rights First, 2022). https://humanrightsfirst.org/wp-content/uploads/2022/12/Digital-Soldiers_QAnon-Report.pdf.

¹⁵³ J. Blazakis, M. El Shawesh, N. Fink, L. McClintock, M. Saltskog, and Z. Schwitzky, *Quantifying the Q conspiracy: A Data-Driven Approach to Understanding the Threat Posed by QAnon* (The Soufan Center, 2021). <https://thesoufancenter.org/research/quantifying-the-q-conspiracy-a-data-driven-approach-to-understanding-the-threat-posed-by-qanon/>; Michael Jensen and Sheehan Kane, "QAnon-Inspired Violence in the United States: An Empirical Assessment of a Misunderstood Threat," *Behavioral Sciences of Terrorism and Political Aggression*, 2021.

dedicated QAnon followers claim to be direct allies with the military, whereby these QAnon adherents serve as a “digital army” that spreads information while the real military prepares for covert intervention in the issues brought to light by the narrative. The social media accounts of both QAnon and its followers have frequently instructed the digital army to use meme warfare to spread disinformation online and even provide materials for adherents to use on its Telegram channel. This public showing of respect for and trust in the military attracts followers with similar mindsets, including service members and veterans.¹⁵⁴

¹⁵⁴ Human Rights First. (2022). *“Digital Soldiers”: QAnon Extremists Exploit U.S. Military, Threaten Democracy* (Washington, DC: Human Rights First, 2022). https://humanrightsfirst.org/wp-content/uploads/2022/12/Digital-Soldiers_QAnon-Report.pdf: Washington, DC.

5. Sextortion Case Studies

In addition to the cyberexploitation case studies described earlier, the IDA team discovered that sextortion is a prevalent cyberexploitation problem. This section defines sextortion and provides relevant case studies.

A. Sextortion Definition and Relevance to the Department of Defense

Sexual extortion, or sextortion, occurs when a victim is approached online by a perpetrator who threatens to expose the victim's intimate information if the victim does not pay a specified sum of money. In some cases, the perpetrator's threats are predicated upon bluffs that they possess intimate images or videos of the victim; in other cases, the perpetrator genuinely does have access to intimate images or videos of the victim that they can choose to expose if the ransom is not paid.

Sextortion is a cybercrime that affects service members disproportionately in comparison to the general adult population. The FBI reported that civilian victims collectively lost \$13.6 million to sextortion scams in 2021.¹⁵⁵ In comparison, NCIS reported that Department of Navy (DON) personnel lost \$263,270 to sextortion scams in 2021. In that year, there were 343,223 DON personnel, which means that about 0.1% of the total U.S. population worked for the Navy. However, DON personnel paid almost 2% of U.S. citizens' total monetary loss to sextortion in 2021.¹⁵⁶ If 0.1% of the population are suffering 2% of the nations' loss, DON personnel are collectively paying about 20 times more than if they were suffering a loss proportionate to their share of the population.

Cybercriminals view service members, particularly male junior enlisted personnel, as being particularly apt to comply with demands for money. Cybercriminals take advantage of the service members' fear of a career-ending mistake by generating a false situation that, if real, would threaten the service member's career and livelihood. Also, even if certain cybercriminals do not intentionally target service members, young men and teenagers are currently the ideal targets for online sextortion operations due to their increased use of gaming platforms, apps, and social media

¹⁵⁵ Federal Bureau of Investigation, San Diego. (2022). "San Diego FBI Warns of Increase in Sextortion Schemes Targeting Young Boys." <https://www.fbi.gov/contact-us/field-offices/sandiego/news/press-releases/san-diego-fbi-warns-of-increase-in-sextortion-schemes-targeting-young-boys>

¹⁵⁶ Naval Criminal Investigative Service. (2021). "A Review of Department of Navy Sextortion Trends: Fiscal Years 2019–2021."

sites relative to young women of a similar age range.¹⁵⁷ This is a demographic disproportionately well represented in the military, as well as in service members' families.¹⁵⁸

B. Cybercriminal Strategies

Not all criminals who conduct successful sextortion operations are sophisticated hackers with state sponsors and ample resources. These cybercriminal operations are relatively easy to conduct as entry barriers are so low. In fact, anyone with access to a cell phone or computer is able to conduct an effective sextortion operation. This section will discuss the different strategies sextortion cybercriminals commonly use and the demographic characteristics that make service members vulnerable to these strategies. In the following section, the emerging threat of deepfake-enabled sextortion is discussed in detail.

1. Fake Child Pornography Strategy

Prisoners in South Carolina's Lee Correctional Institution, a high-security men's state prison, successfully extorted hundreds of thousands of dollars from military personnel across the country from 2016 to 2018.¹⁵⁹ The prisoners used smuggled-in cell phones to pose as young women on dating apps. When they would match with service members on these dating apps, the inmates would turn the conversation to sexual topics within a few hours of texting. Then they would find nude images of women and send them to the service members, often soliciting nude images in return. Once the service member responded, the tone of the conversation would abruptly change. Switching characters, the prisoner would then call the service member, pretending to be the enraged father of the young woman that the service member believed he had been talking to. The father character would inform the service member that the young woman was actually underage, not 18 or 19 as her dating profile had claimed, which meant that the service member was in possession of what seemed to be child pornography. The father character would then threaten to tell the service member's commanding officer or press charges with the local police, unless the service member agrees to send money. The father character would claim that the money will pay for his traumatized daughter's counseling services or replace her phone with an uncontaminated one. Sometimes, the father character in the scenario was replaced or supported by a lawyer or police officer character. If the inmates did not achieve the desired effect immediately, they would continuously call and harass the service member for days. The service member, threatened with

¹⁵⁷ Department of Homeland Security. Immigrations and Customs Enforcement. "Sextortion – It's More Common Than You Think." <https://www.ice.gov/features/sextortion>

¹⁵⁸ Department of Defense (DoD), Office of the Deputy Assistant Secretary of Defense for Military Community and Family Policy (ODASD (MC&FP)). "2020 Demographics – Profile of the Military Community." <https://download.militaryonesource.mil/12038/MOS/Reports/2020-demographics-report.pdf>

¹⁵⁹ <https://www.justice.gov/usao-sc/pr/south-carolina-inmate-sentenced-federal-prison-role-military-sextortion-scheme-1>; <https://www.nytimes.com/2018/11/28/us/south-carolina-inmates-sextortion.html>.

dishonorable discharge or arrest, would transfer money to nonincarcerated accomplices, who would take a cut for themselves and then transfer the remainder into the prisoners' accounts. After initial payments were made, other prisoners would call the victim from different phones, impersonating police officers and threatening arrest if additional payments were not sent.¹⁶⁰

One of the inmates engaged in conducting the sextortion scheme, Wendell Wilkins, was incarcerated and serving a 12-year sentence at the Lee Correctional Institution for attempted armed robbery. Wilkins used the fake child pornography scheme to target military members and threatened them with dishonorable discharge and arrest. From February 2016 through January 2018, Wilkins received at least \$74,000.00 in extorted funds, which investigators traced to at least 25 military victims.¹⁶¹ Another conspirator, Dexter Lawrence, was serving a 22-year sentence for armed robbery and carjacking. Lawrence participated in the scheme from March 2016 to May 2017, gathering a total of \$60,004.09 from at least 25 victims.¹⁶² In total, the South Carolina prisoners and their accomplices were able to extort more than \$560,000 from 442 service members across the country. Their victims spanned the Army, Navy, Air Force, and Marine Corps. According to the U.S. Attorney's Office, several of the service members victimized by this sextortion scheme committed suicide.¹⁶³

The Naval Criminal Investigative Service (NCIS) reported that about 30% of DON personnel victimized by sextortion before May 2021 fell for scams following this child pornography threat playbook. This sextortion scheme was incredibly low-tech and run by people with virtually no resources inside of a prison, yet they were able to successfully target members of the Armed Forces, resulting in multiple deaths. The South Carolina inmates' success raises concerns about the level of success a state-sponsored and well-funded sexual extortion operation might achieve.

2. Fake Webcam Hacker Strategy

Scammers have sent service members emails claiming to have hacked into the service member's computer, accessed the webcam, and recorded an embarrassing video of the service member.¹⁶⁴ Most often, the scammer claims to have a webcam video and screen recording of the victim accessing a pornographic website. The scammer threatens to send this video to the service member's entire contact list and post it on the service member's own social media accounts. The

¹⁶⁰ Ibid.

¹⁶¹ <https://www.justice.gov/usao-sc/pr/south-carolina-inmate-sentenced-federal-prison-role-military-sextortion-scheme>.

¹⁶² <https://www.justice.gov/usao-sc/pr/south-carolina-inmate-sentenced-federal-prison-role-military-sextortion-scheme-1>.

¹⁶³ <https://www.washingtonpost.com/nation/2019/05/14/veterans-suicide-was-blamed-depression-then-police-found-threatening-texts-sent-prison/>.

¹⁶⁴ <https://www.dvidshub.net/news/296868/us-army-cid-beware-hijacked-webcam-scams>.

email often includes one of the service member's passwords to lend legitimacy to the claim; the scammer would have obtained the password via a data breach or mass purchase off the dark web. Alternatively, the scammers spoof their email to make it appear as if it is coming from the service member's email account, lending credence to the idea that a hacker is accessing the service member's entire network and computer. The scammers claim they will delete the video and leave the service member alone if they pay a ransom in Bitcoin.¹⁶⁵ The ransom usually ranges from \$1,000 to \$2,000, and the service member is given a time limit for payment; the added pressure negatively affects the service member's decision-making ability. The scammers intentionally choose an initial ransom amount that is not too exorbitant to convince the service member that it would be easier to just pay the ransom rather than risk the embarrassment. However, once the service member makes the payment, the scammers then begin a constant harassment campaign for additional payments. The psychological badgering associated with sextortion can have tragic mental health consequences.

3. Nude Photo Solicitation Strategy

On May 3, 2023, the U.S. Attorney for the Western District of Michigan indicted three Nigerian men for the sexual extortion of numerous young men and boys across the United States.¹⁶⁶ Their sextortion campaign culminated in the suicide of a 17-year-old boy named Jordan DeMay, who died of a self-inflicted gunshot wound on March 22, 2022 in Marquette, Michigan. The defendants, who were 19, 20, and 22 years old, conducted the scam from Lagos, Nigeria. The grand jury alleges that the defendants purchased hacked social media accounts that they used to pose as young women and directly message teenage and young adult males to lure them into sexual chats. The indictment stated that, "After initiating chat conversations with the victims, the defendants simultaneously used Google and other online applications to research information about the victims, including where the victims lived, where they went to school or worked, and who their family and friends were."^{167,168} The indictment describes how the defendants solicited sexually explicit images of the victims, which they then used to create collages that included other images of the victims, their families and friends, and their schools. The defendants demanded money in exchange for not sharing these collages on social media. When Jordan DeMay was not able to afford the ransom, the scammers threatened him and encouraged him to kill himself, which

¹⁶⁵ Bitcoin is anonymous and untraceable, so the victim has no avenue to refund their money, and the authorities cannot find who is responsible. Bitcoin is also ideal for untraceable international money transfers, and many of these scams are being conducted from African and Asian countries.

¹⁶⁶ https://www.justice.gov/usao-wdmi/pr/2023_0503_Sextortion_Indictment.

¹⁶⁷ Ibid.

¹⁶⁸ Even if the victims had had very private online accounts, the scammers could still have purchased this information from data brokers. The indictment does not make clear whether the criminals accessed the victims' information via public social media accounts or purchased it via data brokers.

he did. The FBI worked with Nigerian law enforcement to arrest the defendants, who are facing extradition to the United States.¹⁶⁹ In 2022, two other American 17-year-old boys, Gavin Guffey and Ryan Last, also committed suicide immediately after becoming victims of sexual extortion.¹⁷⁰ Of the 3,000 minor victims of online sextortion in 2022, more than a dozen died by suicide.¹⁷¹ The high prevalence of minors being victimized by sexual extortion demonstrates that this threat is not only relevant to young service members, but also to the teenage children of older service members.

4. Demographic Vulnerabilities

The three 17-year-old American boys who committed suicide in 2022 are in the same generation and demographic as thousands of current and future U.S. service members. Their deaths are illustrative of this demographic's vulnerability to online scams of a sexual nature, a vulnerability that cybercriminals are actively exploiting. Recently, young Americans have become increasingly vulnerable to online sexual scams partly because of major declines in their engagement in in-person romantic relationships. From 2000 to 2018, the percentage of men aged 18 to 24 who report engaging in absolutely no sexual activity for the past year increased from 18.9% in 2000 to 30.9% in 2018.¹⁷² Among men aged 25 to 34 years, the sexual inactivity doubled from 7.0% in 2000 to 14.1% in 2018. This study was completed in 2020, and the last survey data was taken in 2018. Over the five years since this survey was conducted, the pandemic and other trends of social isolation have likely caused this sexual inactivity to continue its upward trend. Young men in the United States—young service members being no exception—are, as a result, incredibly susceptible to these sextortion schemes. Strange online interactions with women who quickly turn the conversation to sexual topics may not raise as many red flags today as they may have 10 years ago. The previous generation of service members statistically participated in more romantic relationships, had more experience with the way women usually communicate, and may have been able to spot the impersonation faster. These demographic characteristics that make young service members vulnerable to sextortion also apply to the teenage sons of older service members. Targeting the teenage sons of military leaders would be an effective way for state-sponsored cybercriminals to destabilize the leaders' lives, especially if their goal is not monetary gain but to induce the young men and boys to commit suicide.

Because of how frequently young service members relocate to new places, they are even more likely to seek human connection online than their civilian counterparts. Also, young service members have a steadier income in comparison with the college student demographic that makes

¹⁶⁹ https://www.justice.gov/usao-wdmi/pr/2023_0503_Sextortion_Indictment.

¹⁷⁰ <https://www.cnn.com/2022/05/20/us/ryan-last-suicide-sextortion-california/index.html>.

¹⁷¹ <https://www.fbi.gov/news/press-releases/press-releases/fbi-and-partners-issue-national-public-safety-alert-on-financial-sextortion-schemes>.

¹⁷² <https://jamanetwork.com/journals/jamanetworkopen/article-abstract/2767066>.

up a large portion of the 18- to 24-year-old population. Scammers know that service members are more likely to be able to afford ransom payments and may be more likely to comply with a demand for ransom when faced with the threat of an incident being reported to their commanding officer. College students are not faced with similar authority structures or potential penalties. There has been a spike in cases where the perpetrators impersonate a member of the victim's chain of command to encourage payment.¹⁷³ The increase in sextortion-related suicides in 2022 is demonstrative of the need to increase troops' threat awareness, especially for single service members who are on dating apps or who would be the most likely to respond to direct messages from people posing as interested women online. Once sexual images are exchanged, the scammers have the upper hand.

The most menacing sextortion scams are those in which the scammer has successfully obtained sexually explicit images of the victim and is not simply bluffing about the possession of such material. In the majority of sextortion-related suicide cases, the scammers did indeed possess the victim's images. Most of the time, however, sextortion scammers do not follow through on their threats to expose the victim's sexually explicit images. In a threat awareness message posted in May 2021, NCIS reported that 92% of all sextortion perpetrators did not (or could not) follow through on threats to distribute. In the same message, NCIS reported that from October 2018 to May 2021, they saw only 26 instances of the perpetrator following through and posting the sexually explicit images of DON personnel. However, this frequency may be increasing. In a threat awareness update posted in May 2023, NCIS found that 43% of sextortion victims did not pay the scammers' demands, and "in many of these instances, victims experienced heightened harassment". When the Service member failed to pay, scammers sometimes created social media accounts with the victim's name and image, friended the victim's friends and family, and then posted the victim's explicit photos. In five cases, scammers used these social media profiles to post child pornography. Whether the entire scam is predicated on a lie or the scammer does possess nude images of the victim, sextortion victims suffer serious mental health and financial consequences.¹⁷⁴

C. National Security

Sextortion of service members also poses a national security risk. Cybercriminals are targeting members of the American military from all over the world. According to NCIS, all of the sextortion scams targeting DON personnel seemed motivated by monetary gain alone.¹⁷⁵ None of the victims have reported being extorted for classified documents or unauthorized access to military facilities. However, there are other entities who may note the success of these operations

¹⁷³ Naval Criminal Investigative Service. (2021). "A Review of Department of Navy Sextortion Trends: Fiscal Years 2019-2021."

¹⁷⁴ Ibid.

¹⁷⁵ Ibid.

and will have motivations more nefarious than monetary gain. Adversary governments may seek to distract service members during critical times of geopolitical action, financially destabilize them, and/or extort classified information rather than money. For cybercriminals with non-monetary primary motivations, U.S. service members and their families become ideal sextortion targets.

If state-sponsored cybercriminals wish to distract upper-level military leadership, a smart strategy would be to purchase information about the upper-level leaders' families from data broker websites. They could then use this information to launch targeted sexual extortion campaigns against the leaders' children. Once they establish a rapport with the teens, they can use a variety of strategies to solicit explicit photos that can be used for sextortion. Teen girls are historically targeted with sexual extortion not for money but for the further production of sexually illicit material; teen boys are usually targeted for money. Either motivation can result in victimization over months and years, usually without report to parents or authorities because of extreme embarrassment and fear of the photos' exposure. Both teen boys and girls who have been victimized by sexual extortion have been known to commit suicide as a result of the acute stress. According to the FBI, there were 7,000 reports of sextortion targeting minors in the U.S. in 2021, which resulted in 3,000 victimizations and more than a dozen suicides.¹⁷⁶ Consider the perspective of a state-sponsored cybercriminal who wants to cause major distraction among U.S. senior leadership prior to a major operation by their nation (e.g., invasion of a sovereign nation). The creation of a targeted sextortion campaign against the children of senior leadership would generate the desired distraction, especially if the scammers modify their attack to inflict maximum mental health damage. Since their motivations are not primarily monetary, they are likely going to post/share the images despite payments. Cybercriminals could cast a wide net and target as many teen children of senior leadership that they can identify online, which would increase their chances of causing significant damage to the well-being of some of these children. Also, if the operation is conducted by more experienced cyber actors, they would be able to obscure the location origin of the operation, giving their state sponsor plausible deniability. Even if they aren't able to obscure the country of origin, the government could claim that the actors are cybercriminals acting with no connection to the government and solely for financial gain. The plausible deniability that this strategy allows is very valuable from the adversary's perspective.

Sextortion could also be used to extort classified information, wherein victims are coerced into becoming insider threats. The Air Force Office of Special Investigations has also never received a report of a security breach as a result of sexual extortion. However, if a sextortion victim were to be successfully extorted for classified material, this would create a dangerous feedback loop. Once the service member has violated the Espionage Act, they have lost their avenue for reporting the crime to military authorities without facing prosecution themselves. Past evidence demonstrates that once a victim makes a single financial payment to cybercriminals, the

¹⁷⁶ <https://www.justice.gov/usao-sdin/pr/fbi-and-partners-issue-national-public-safety-alert-sextortion-schemes>.

harassment campaign is almost never-ending. Victims have been revictimized with the same photos years after the original contact. For cybercriminals who seek to extort classified information rather than money, the same persistent tactics would likely create an involuntary insider threat. In this case, the cybercriminals would have a more significant upper hand because, not only do they hold embarrassing sexual images of the victim, they also have knowledge of the victim's violation of the law to hold over them. Unlike many victims of financial sextortion who report the crime after they have already lost their money, a victim in this scenario would have a strong incentive not to report. In the future, cybercriminals may aim to use sexual extortion to compel military personnel to become insider threats, though there is no evidence of this occurring yet.¹⁷⁷

Due to the intimate nature of the crime, sexual extortion is a notably difficult crime for law enforcement to track and fight. Victims are often embarrassed and generally do not report the crime to the police. As such, the statistics on sextortion do not accurately represent the actual prevalence of the crime. Cybercriminals' ability to adapt also creates a significant challenge. They take advantage of emerging technologies to expand their potential victim pool and evade detection.

D. Deepfake-enabled Sextortion

Deepfake technology is mostly discussed in national security circles because of the potential to use synthetic images to spread disinformation and propaganda. However, a discussion of deepfakes and the risks they pose to national security would be incomplete without the discussion of deepfake-created pornography. Deepfake-created pornography is currently being used to sexually harass and extort primarily female victims. The expansion of cybercriminals' sextortion victim pool to include women will likely have particularly pernicious effects for female service members.

1. The Evolution of Deepfaked Pornography

Deepfake technology has been primarily used to create pornographic content since its inception. In 2019, Dutch cybersecurity company Deeptech published a report finding that 96% of all deepfakes online at the time were pornographic in nature.¹⁷⁸ Deepfake technology is still primarily used to create pornography, and these creators operate and evolve within an ethically dubious and unregulated realm.

The popularity of these deepfake pornography sites illustrates the broader trend of personalized online content. What was once a market only of explicit videos of attractive women evolved to include synthesized explicit videos of audiences' favorite actresses and celebrities. Audiences could submit requests for their favorite celebrities to be featured, and more niche celebrities were featured over time. The initial wave of deepfake pornography featured A-list

¹⁷⁷ Personal communication with Air Force Office of Special Investigations.

¹⁷⁸ https://regmedia.co.uk/2019/10/08/deepfake_report.pdf.

actresses and household names. As deepfaked pornography continued to evolve, lower-profile Internet celebrities, such as women who film themselves playing video games, started seeing their likenesses featured in videos without their consent. One such woman, famous for streaming video games, became aware of her image being used for deepfaked pornography videos that were circulating the Internet.¹⁷⁹ However, the woman was unable to prevent the videos' widespread circulation. Internet trolls sent the videos to her family members, some of whom were older, very religious, and did not believe that the videos were fabricated despite the young woman's explanations. She endured significant online sexual harassment and dealt with significant emotional distress as a result, which was compounded by the lack of available legal recourse.¹⁸⁰

On the social networking site Discord, deepfake pornography creators began selling five-minute pornographic deepfakes featuring the "personal girl" of the customer's choice. These videos cost between \$25 to \$65 each, and the "personal girl" refers to anyone with fewer than two million Instagram followers.¹⁸¹ However, the present-day boom of consumer-friendly deepfake creation apps will likely undermine these creators' business models. Using the new apps, people are now able to easily make videos for a fraction of the cost. One such app advertised its services using a widespread campaign across Meta's Facebook and Instagram in March 2023. Within the app, users choose a video template or upload a (presumably pornographic) video of their own choice. Then, "users can input a single photo of anyone's face, and receive a face-swapped version of the video in seconds."¹⁸² This particular app, developed by Ufoto Limited, was advertised widely across Meta's platforms. Ufoto Limited is owned by the parent company Wondershare, which is headquartered in Shenzhen, Guangdong, China.¹⁸³ Following NBC News' reporting on the ad campaign, Meta brought the ads down, Apple removed the app from the App Store (where it had been available for ages 9 and up), and Google removed it from the Google Play store. However, similar apps remain available. This ad campaign and the rapid emergence of such apps illustrates how thoroughly this once-advanced technology has permeated into mainstream corners of the Internet.

These mainstream corners of the internet are struggling to regulate and enforce regulations of deepfaked pornography on their platforms. Twitter's nonconsensual nudity policy bans "images or videos that superimpose or otherwise digitally manipulate an individual's face onto another

¹⁷⁹ www.wired.com/story/deepfakes-twitch-streamers-qtcinderella-atric-pokimane/.

¹⁸⁰ Ibid.

¹⁸¹ <https://www.nbcnews.com/tech/internet/deepfake-porn-ai-mr-deep-fake-economy-google-visa-mastercard-download-rcna75071>.

¹⁸² Hao, Karen. (2021). "A Horrific New AI App Swaps Women into Porn Videos with a Click." MIT Technology Review. <https://www.technologyreview.com/2021/09/13/1035449/ai-deepfake-app-face-swaps-women-into-porn/>

¹⁸³ Meanwhile, deepfake creation within China is highly regulated. Chinese regulations prohibit the production of deepfakes without the subjects' consent and require all deepfakes to be clearly labelled as synthetic material.

person's nude body.”¹⁸⁴ However, the policy states that the individual depicted in the deepfake, or a representative, may need to contact Twitter to get the content brought down.¹⁸⁵ Graphic deepfakes of young women who are popular on TikTok, particularly Addison Rae Easterling and Charli D'Amelio (ages 22 and 19, respectively), are garnering millions of views on Twitter. The content is remaining on the site for weeks at a time before being removed.¹⁸⁶

2. Deepfaked Pornography Used for Online Sexual Harassment and Extortion

a. Online Sexual Harassment

Deepfaked pornography is not solely created for the fantasy-fulfillment purposes described above. Creators also make deepfaked pornography to degrade and demean women who have angered them. In April 2018, an investigative journalist in India named Rana Ayyub was informed by a source that her face had been used in a pornographic deepfake. The video, which was sometimes accompanied by rape threats and her home address, circulated to thousands on Facebook, Twitter, and WhatsApp.¹⁸⁷ Another woman, feminist media critic Anita Sarkeesian, found out her likeness was used to create a particularly degrading pornographic deepfake video, which was subsequently viewed more than 30,000 times on the pornographic website Pornhub. Ayyub and Sarkeesian's experiences illustrate the negative impact that such sexual deepfakes can have, essentially serving as character assassinations with no form for prevention or recourse. The stakes rise even higher when these offenders know the women in real life, attach her location to her synthesized image, and threaten to blackmail her with these images.

b. Sexual Extortion

Before deepfakes existed, cybercriminals had to successfully obtain (or convince victims that they possessed) nude images of their victims before sexually extorting them, which meant the victim pool mainly consisted of people who could be convinced to share nude images. This precluded most women and married men from inclusion. It is generally more difficult to convince women to share nude images with strangers than young men, and older, often married male service members with higher incomes do not frequently expose themselves to opportunities for sextortion. However, with the emergence of cheaper, more ubiquitous, and more convincing deepfake technology, cybercriminals are able to threaten to release graphic content depicting victims outside the original pool. Generative AI has advanced to the point where it is very difficult to determine with the naked eye if an image or video is synthetic. Deepfakes will only continue to improve,

¹⁸⁴ <https://help.twitter.com/en/rules-and-policies/intimate-media>.

¹⁸⁵ Ibid.

¹⁸⁶ <https://www.nbcnews.com/tech/internet/deepfakes-twitter-tiktok-stars-rcna87295>.

¹⁸⁷ <https://www.washingtonpost.com/technology/2018/12/30/fake-porn-videos-are-being-weaponized-harass-humiliate-women-everybody-is-potential-target/>.

which gives cybercriminals the ability to threaten victims with synthetic videos that are almost impossible to distinguish from genuine videos.

There are many possible contingencies for the use of deepfake technology for purposes of sexual extortion. Anyone who has posted their face online is now potentially exposed to victimization. Cybercriminals can create the sexual deepfakes, send them to the victim, and threaten widespread circulation. Exposure to coworkers, friends, and family will have severe consequences for the victim regardless of the authenticity of the images or video, and it can be very difficult to convince others that the images or video are not real, especially when the others are older, not as technologically literate, or did not look at the image very closely. As such, fake images can have real career and reputational consequences. In addition to workplace embarrassment, the exposure of this faux online sexual activity may ostensibly threaten someone's relationship.

c. Relevance to Servicewomen

Before the emergence of deepfake-enabled sextortion, sexual extortion schemes were relevant to the DoD because they successfully target young male service members. However, pornographic deepfakes historically almost exclusively target women (99% of pornographic deepfakes online).¹⁸⁸ As previously stated, it is much more difficult to convince a woman to send a nude photograph to a stranger than it is to convince a young man to do the same. The use of sexual deepfakes to evade this obstacle and sexually extort women is not merely anticipated, it is already occurring. On June 5, 2023, the FBI's Internet Crime Complaint Center released a public service announcement about this emerging threat: "[T]he FBI continues to receive reports from victims, including minor children and non-consenting adults, whose photos or videos were altered into explicit content. The photos or videos were then publicly circulated on social media or pornographic websites, for the purpose of harassing victims or sextortion schemes...As of April 2023, the FBI has observed an uptick in sextortion victims reporting the use of fake images or videos created from content posted on their social media sites....".¹⁸⁹ Cybercriminals are already beginning to incorporate sexual deepfakes into their sextortion campaign strategies, and it is likely only a matter of time before service members are targeted in this way, if they have not been already.

The non-consensual circulation of nude images of active-duty servicewomen in the past demonstrates the elevated risk for servicewomen victimized by sextortion. Consider the events that took place surrounding the Marines United Facebook page in 2017. The Marines United page was an invite-only Facebook page that limited membership to men who were active duty or veterans of the U.S. Marine Corps, U.S. Navy, or British Royal Marines. It had 30,000 members.

¹⁸⁸ https://regmedia.co.uk/2019/10/08/deepfake_report.pdf.

¹⁸⁹ Federal Bureau of Investigation. (2023). "Malicious Actors Manipulating Photos and videos to Create Explicit Content and Sextortion Schemes." Alert Number I-060523-PSA, June 5. <https://www.ic3.gov/Media/Y2023/PSA230605>

The page encouraged members to contribute to a Google Drive photo-sharing service that held hundreds of images of female service members in various stages of undress. Some of the photos were taken by the women themselves and shared non-consensually; others were surreptitiously taken by members of the Facebook page of the women in uniform, performing their daily duties on base. These photos would then be posted with vulgar and degrading captions, often eliciting comments along the same vein.¹⁹⁰ The drive was categorized by folder, with some folders containing the full name, rank, and military station of the victim. More than two dozen women had their full name, rank, and location linked to their photographs in the Google Drive. The photos were often supplemented with screenshots of the victims' social media pages. Naturally, such details exposed the victims to further sexual harassment, unwanted contact, and stalking.¹⁹¹ One of the women was photographed bending over to pick up equipment at Camp Lejeune, and she was not aware of the photograph's circulation and commentary until approached by reporters once the scandal broke. One of the women found out from a male coworker that her nude photos were on the site. Another woman, a civilian who had previously dated a Marine, said she felt the need to move to get a fresh start after images of her were posted on the page, and she was subsequently harassed at her place of work by men who had seen the images.¹⁹² While men who have been sextorted are embarrassed if cybercriminals post their intimate images on social media, the chances that multitudes of men or women (coworkers, supervisors, service members across the country) will save the images to a centralized database, connect the images to name/rank/location, make vulgar comments, and systematically circulate the images are incredibly low. In contrast, women facing the same threats will likely look at the Marines United case and fear their images, if posted, may follow them throughout their career, lead to in-person sexual harassment, and be looked at across the country.

¹⁹⁰ <https://revealnews.org/blog/hundreds-of-marines-investigated-for-sharing-photos-of-naked-colleagues/>.

¹⁹¹ <https://www.marinecorpstimes.com/news/pentagon-congress/2017/03/06/i-don-t-want-to-leave-my-house-victims-haunted-by-marines-nude-photo-scandal/>.

¹⁹² <https://www.marinecorpstimes.com/news/pentagon-congress/2017/03/06/i-don-t-want-to-leave-my-house-victims-haunted-by-marines-nude-photo-scandal/>.

6. The Role of Social Media in Cyberexploitation

Today, what happens online increasingly affects what happens offline. Alternative (non-mainstream) media sources and social media sites are platforms for information meant to broaden and deepen existing political and social divisions. Advancements in technologies, such as generative AI networks and deepfakes, facilitate the spread of misleading or malicious information and make it very difficult to determine what is real and what is fabricated. This online landscape is rife with opportunities for attempted exploitation, particularly for service members and their families.

A. Navigating a “Post-Truth” World

The concept of a “post-truth” world has gained prominence in recent years; the Oxford Dictionary selected *post-truth* as the word of the year in 2016 and defines it as “relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief.”¹⁹³ The post-truth world is characterized by the following:^{194,195,196,197}

1. The prevalence of misinformation and disinformation:¹⁹⁸ The spread of misinformation and disinformation is rampant in a post-truth world. False or misleading information can easily circulate through social media and alternative media sources. Manipulation tactics such as deepfakes and bots can amplify the effect of false narratives.
2. Emotional appeals over factual evidence: Emotional responses drive engagement with post-truth narratives. Stoking fear or anger is a powerful tool for attracting attention and

¹⁹³ “Post-truth,” *Oxford English Dictionary*, https://www.oed.com/dictionary/post-truth_adj?tab=meaning_and_use#1217123470.

¹⁹⁴ A review of educational responses to the “post-truth” condition: Four lenses on “post-truth” problems, 55:3, 107-119, DOI: 10.1080/00461520.2020.1786388

¹⁹⁵ Truth Decay and National Security. <https://www.RAND.org/blog/2023/08/truth-decay-and-national-security.html>.

¹⁹⁶ Post-Truth and the Search for Objectivity: Political Polarization and the Remaking of Knowledge Production. <https://estsjournal.org/index.php/ests/article/view/286>.

¹⁹⁷ “Democracy and Fake News: Information Manipulation and Post-Truth Politics.” https://www.researchgate.net/publication/342946132_democracy_and_fake_news_information_manipulation_and_post-truth_politics.

¹⁹⁸ Misinformation refers to unintentionally false information; disinformation comprises intentionally false or misleading information.

swaying individual and public opinion, even in the face of contradictory factual evidence.

3. Loss of trust in institutions: Post-truth discourse often emerges following a widespread loss of trust in institutions such as governments, mainstream media organizations, and scientific establishments.
4. Devaluation of expertise and authority: In a post-truth world, expertise and authoritative sources of information are often undermined or dismissed. Rejecting these sources can stem from anti-establishment sentiments, ideological biases, or a belief that experts support a conspiratorial agenda.
5. Weaponization of information: In a post-truth landscape, information becomes a weapon for manipulation and control.
6. Polarization and tribalism: Post-truth dynamics tend to exacerbate social and political polarization as individuals gravitate toward like-minded communities. This further entrenches divisions and makes it harder for separate groups to find common ground.

It is important to note that post-truth does not mean that truth no longer exists or that all information is equally valid. Instead, the concept of post-truth highlights the challenges posed by the manipulation of information and the erosion of trust in traditional institutions. Navigating a post-truth world requires critical thinking skills, media literacy, and a commitment to evidence-based reasoning.

The post-truth era has ushered in new national security challenges. Currently, public trust in the government and other traditional institutions is low, which has created an audience primed for misleading or fabricated information meant to exacerbate that distrust or incite anger or fear. Established and emerging technologies have made it easier to create and disseminate this information. Social media sites enable users to seek out beliefs and ideologies similar to their own and encourage trust in sources that are ideologically familiar but otherwise untrustworthy or malicious. Service members are generally online more often than the general population, which places them at greater risk of attempted exploitation and/or radicalization.

B. Social Media

Social media has a significant role in the military community. It provides helpful connections, giving military families a means to navigate moves to new locations and strengthening family bonds during periods of separation due to training or deployment. Active duty military members, on average, spend more time on social media than the general population (see Figure 6-1). This is also partly due to demographics: The majority of service members are Millennials or Generation Z,¹⁹⁹ and are thus used to spending much of their lives online.

¹⁹⁹ <https://www.cfr.org/background/demographics-us-military>.

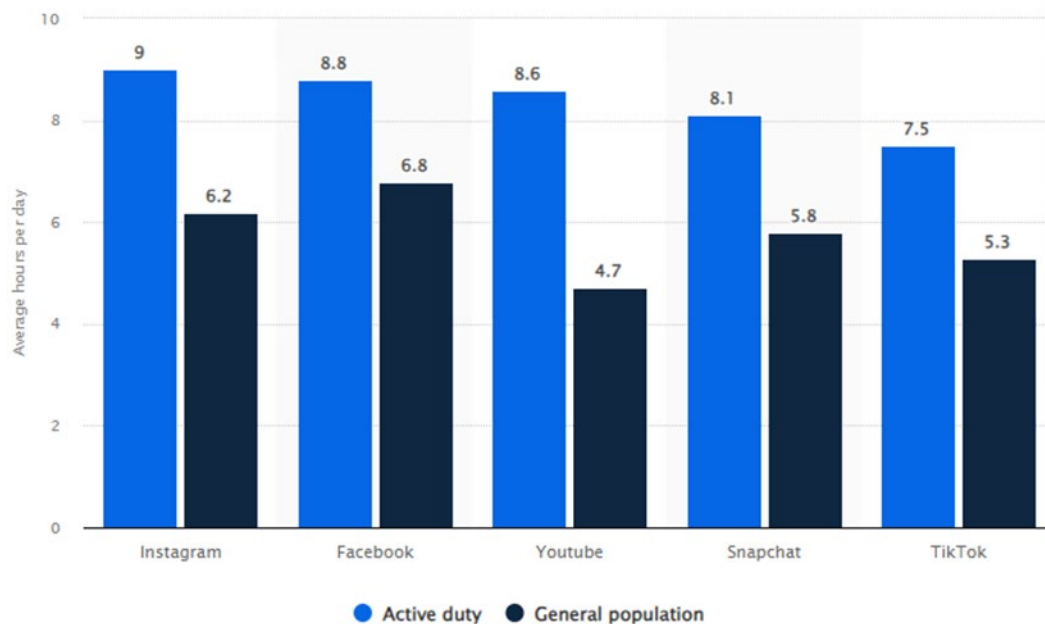


Figure 6-1. Social Media Use by Active Military and the General Population²⁰⁰

DoDI 8170.01, “Online Information Management and Electronic Messaging,” provides guidance on social media use,²⁰¹ and DoDI 5400.17, focuses on official social media accounts associated with the DoD and Military Services.²⁰² The Services have issued their own policies as well.²⁰³ Though these documents specify rules and regulations for using social media, they do not fully address the risks of social media use. Service members are discouraged from posting information directly related to their jobs, but even seemingly benign posts on social media could endanger service members by “revealing their locations, security measures, mission operations, or troop movements.”²⁰⁴ Posts by military spouses about deployment times could damage operational

²⁰⁰ Stacy Jo Dixon, “Average Number of Hours per Day Spent on Select Social Media Platforms by Active-Duty Military Members in the United States as of February 2020,” *Statista*, 2022, <https://www.statista.com/statistics/1130021/hours-spent-social-media-us-active-duty-military-members/>

²⁰¹ Office of the Chief Information Officer, DoDI 8170.01, “Online Information Management and Electronic Messaging,” January 2, 2019, https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Personnel_Related/22-F-0350_DODI_8170.01-Online_Information_Management_and_Electronic_Messaging_2Jan2019_CH-1_24Aug2021.pdf.

²⁰² Office of the Assistant Secretary of Defense for Public Affairs, DoDI 5400.17, “Official Use of Social Media for Public Affairs Purposes,” August 12, 2022, <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/540017p.PDF>.

²⁰³ See <https://www.defense.gov/social-media-policy/> for links to Service social media policies.

²⁰⁴ <https://www.military.com/deployment/maintaining-operational-security-with-social-media.html>.

security.²⁰⁵ Information voluntarily posted on social media could be co-opted for malicious purposes. In 2018, social media posts surfaced claiming that a U.S. service member had killed a Polish soldier and stolen a car. The fabricated posts referenced the service member's unit and featured photos that he had posted to social media.²⁰⁶

Social media algorithms prioritize data sharing to promote engagement, which amplifies targeting opportunities. For instance, a user's ethnicity, political beliefs, financial well-being, and even medical information can be found and delivered to interested parties for a fee.²⁰⁷ Service members and veterans represent a lucrative market, with spending power of \$1.3 trillion (and growing).^{208,209} Advertisers clamor for data on this market, and social media companies have responded by creating algorithms that can accurately predict the identity of service members. Advertisers are then able to use this information to tailor ads to service members and veterans, often pushing ads that celebrate military holidays and offer special discounts. Clicking on an ad helps verify that the targeted account is real.²¹⁰ Social media companies also use this information to refine their algorithms and identify networks and purchasing patterns, and they employ cookies to ensure information is recorded even after a service member has logged out of their account.²¹¹

The reams of information gathered by social media sites and data brokers (companies that collect and aggregate personal data to sell) enable precise targeting for advertisers or potential scammers and increase service members' vulnerability to threats. In 2014, an ISIS spokesperson encouraged followers to use social media to collect information on service members, including home addresses. Followers were then urged to show up at service members' homes and slaughter them.^{212,213} In 2015, Terrence McNeil, a professed ISIS supporter, posted the names and addresses of 100 service members, along with dozens of photographs, on Tumblr. McNeil's post attempted

²⁰⁵ Ibid.

²⁰⁶ <https://www.military.com/daily-news/2020/08/16/fake-news-wreaking-havoc-battlefield-heres-what-militarys-doing-about-it.html>.

²⁰⁷ <https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government>.

²⁰⁸ <https://www.adweek.com/sponsored/3-things-you-need-to-know-about-marketing-to-the-military/f>.

²⁰⁹ <https://www.refuelagency.com/military-marketing-outdoor-brands/#:~:text=There%20are%2040%20million%20military,power%20and%20increasing%20consumer%20influence.>

²¹⁰ [https://www.marketingtechnews.net/news/2016/aug/16/social-identity-verification-industries-need-catch/.](https://www.marketingtechnews.net/news/2016/aug/16/social-identity-verification-industries-need-catch/)

²¹¹ <https://www.marines.mil/Portals/1/Docs/Social-Media-Handbook20170308.pdf>.

²¹² <https://apps.dtic.mil/sti/trecms/pdf/AD1085340.pdf>.

²¹³ <https://commons.erau.edu/cgi/viewcontent.cgi?article=1000&context=pr-honors-csi>.

to incite violence against the named service members.²¹⁴ The information came from a hack of another website.

Social media algorithms can also be exploited to target service members and exploit their vulnerabilities to drive engagement with disinformation campaigns and extremist ideologies. The algorithms learn from user engagement and behavior: If a service member clicks on a particular post, the algorithm driving content selection will then generate a series of posts on related topics. This targeting is further enhanced using factors such as location, demographics, interests,²¹⁵ and even race or gender.²¹⁶ Even if this information was used for benign purposes, it could still lead to unintentional racial or ethnic targeting. For an adversary looking to exploit existing divisions and sow false narratives, this type of information is very useful. For example, researchers at Duke University found about 3,500 examples of Russian-generated social media content used to influence U.S. audiences between 2015 and 2017. The campaign focused a great deal of resources targeting veterans and the Black community. Veterans were fed posts attempting to radicalize them and convince them to commit acts of domestic violence during the 2016 elections. The Black community was targeted with posts meant to dissuade them from heading to the polls.²¹⁷

Regarding social media use, the challenge for service members and their families is balancing the need for connection (and the morale-boosting effects that result) and the overall safety of service members, their families, and their units.

C. Machine-Manipulated Media (i.e., Deepfakes)

The 2021 NDAA defined machine-manipulated media as “video, image, or audio recordings generated or substantially modified using machine learning techniques in order to, with malicious intent, falsely depict the speech or conduct of an individual without that individual’s permission.” These media are known colloquially as *deepfakes*.

Deepfakes are forged images, audio, and video created using generative AI technologies²¹⁸ that may be indistinguishable from authentic content. Deepfakes should not be confused with “cheapfakes,” which comprise content edited or manipulated through traditional avenues (e.g., editing with Photoshop software). Deepfakes were created in 2017 by a Reddit user, who grafted

²¹⁴ <https://www.longwarjournal.org/archives/2017/04/ohio-man-pleads-guilty-to-terror-charges-after-posting-islamic-state-hit-list.php>.

²¹⁵ <https://developers.facebook.com/docs/app-ads/targeting>.

²¹⁶ <https://dl.acm.org/doi/pdf/10.1145/3437963.3441801>.

²¹⁷ <https://dukespace.lib.duke.edu/dspace/bitstream/handle/10161/27083/AMBUSH%20ON%20BLACK%20VETERANS.pdf?sequence=1>.

²¹⁸ Congressional Research Service. Deep Fakes and National Security. <https://crsreports.congress.gov/product/pdf/IF/IF11333/7>. April 17, 2023

pictures of celebrity faces onto actors' bodies. These initial versions were obviously fake and both expensive and arduous to create. However, new technologies have lowered the barrier to entry and have made it much more difficult to discern between deepfakes and authentic media.

Initially, deepfakes were created by a form of AI called generative adversarial networks (GAN). Within GANs, two AI networks compete with each other. A creator network generates an image and a judge network determines how realistic the image is and provides feedback to the creator network, which adjusts the image accordingly. This establishes a feedback loop that allows GANs to produce increasingly realistic images without human involvement.²¹⁹

Currently, the most popular method for creating deepfakes is stable diffusion, a generative AI text-to-image technology. Stable diffusion models are able to create detailed representations using a brief text description:²²⁰ for example, a user could request an image of an apple that looks like its painted in the style of Van Gogh's *Starry Night* or an image of an American teenager waving a Russian flag in the middle of Times Square that looks like a photograph. Anyone with a low level of computer literacy can easily access and use AI image generators—Midjourney for example²²¹—for little to no cost. This ease of access means deepfakes will increasingly be used for purposes ranging from comedic to criminal.

Deepfakes are becoming popular tools for extortion. “Deepnude” deepfake technology has been used to remove the clothes from pictures of women, which are then used to discredit or financially extort them.²²² In June 2023, the FBI published a public service announcement warning of the dangers of deepfake extortion. The announcement stated that, “As of April 2023, the FBI has observed an uptick in sextortion victims reporting the use of fake images or videos created from content posted on their social media sites or web postings, provided to the malicious actor upon request, or captured during video chats. Based on recent victim reporting, the malicious actors typically demanded: (1) Payment (e.g., money, gift cards) with threats to share the images or videos with family members or social media friends if funds were not received; or (2) The victim send real sexually-themed images or videos.”²²³

Additionally, deepfake audio has been used to extort money through ransom scams. During these scams, the scammer creates deepfake audio of an individual's voice to use as proof of

²¹⁹ See <https://medium.com/analytics-vidhya/gans-a-brief-introduction-to-generative-adversarial-networks-f06216c7200e> for an explanation of GANs.

²²⁰ See <https://stable-diffusion-art.com/how-stable-diffusion-work/> for more information about stable diffusion models.

²²¹ See <https://www.midjourney.com/>.

²²² Matt Burgess, “A Deepfake Porn Bot Is Being Used to Abuse Thousands of Women,” | *Wired*, October 2020, <https://www.wired.com/story/A-Deepfake-Porn-Bot-Is-Being-Used-to-Abuse-Thousands-of-Women/>.

²²³ Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes, <https://www.ic3.gov/media/y2023.psa230605>.

kidnapping. The scammer calls the victim, plays the recording to convince the victim that a loved one is being held captive, and then asks for ransom money.²²⁴

These extortion scams, sextortion scams in particular, have reached the military (see Section 5 for more information). Other deepfake-enabled threats against the military focus on senior leaders in DoD. As a result of their positions, these leaders are often depicted in images or videos, which can be used to create deepfakes to incite anger against the DoD or put our national security at risk.

²²⁴ A victim of a ransom scam told their story to the IDA research team.

7. Intelligence Assessments

This section provides the intelligence assessments requested by the 2021 NDAA.

A. Cyberexploitation Threats by Foreign Actors Relative to Other Forms of Information Warfare

The IDA team assessed whether cyberexploitation is a substantial threat compared to other means of information warfare (IW), and whether cyberexploitation is an increasing threat. As defined earlier, cyberexploitation encompasses a range of activities conducted and/or capabilities used in the cyberspace domain to abuse, misuse, and manipulate information about service members and their families to benefit the exploiter. IW, though not officially defined in Joint Doctrine, “encompasses the range of offensive and defensive efforts that use information across the competition continuum to exploit the information environment against adversaries, to inform public opinion, and to compel decision makers to take certain actions.”²²⁵ The overlap between the definitions of cyberexploitation and IW suggest that cyberexploitation could be the means to achieving IW ends.

Each U.S. service component organizes and employs information forces in the different manners best suited for their specific mission requirements. The full variety of capabilities, operations, and activities that comprise IW now fall under the umbrella term “operations in the information environment” (OIE). OIE activities include, but are not limited to, key leader engagements, public affairs, civil-military operations, military information support operations, military deception, operations security, electromagnetic spectrum operations, space operations, and cyberspace operations.²²⁶ These military actions affect drivers of behavior to inform, influence, and exploit target audiences while protecting friendly ones; however, adversarial state and non-state actors conduct their own version of OIE against their local populations, as well as against U.S. Armed Forces and their families.

Foreign governments and non-state actors are capitalizing on emerging technologies (e.g., social media) to optimize their OIE tactics, which range from competition, to crisis, and ultimately to conflict. This approach to gaining an asymmetric advantage entertains the concept of winning a conflict without having to fight. Using various methods and techniques, information can be applied and managed in such a manner to best shape a narrative that suits the purposes and goals of that

²²⁵ JP 3-04, III-25. https://jdeis.js.mil/jdeis/new_pubs/jp3_04.pdf

²²⁶ JP 3-04., App B-7.

state actor. In turn, these narratives “can induce long-term effects on an audience’s beliefs, attitudes, and behavior.”²²⁷

B. People’s Republic of China

The DoD’s *2022 Annual Report to Congress on the People’s Republic of China* (PRC) describes how the People’s Liberation Army (PLA) has undergone several modernization efforts, including the establishment of the Strategic Support Force (SSF) in 2015. The SSF is “a theater command-level organization established to centralize the PLA’s strategic space, cyberspace, electronic, information communications, and psychological warfare missions and capabilities.”²²⁸ The SSF Network Systems Department is specifically responsible for the IW mission in support of the Chinese Communist Party’s (CCP’s) practice of political warfare.²²⁹ The scope of the CCP’s OIE has expanded from the analog era of local print media and broadcast radio propaganda to what they have dubbed “intelligentized warfare,” which makes use of advanced technologies to suppress, shape, and control adversary’s decision-making process within a concept called *cognitive domain operations*²³⁰ (a domain that the U.S. DoD first defined in 2001).²³¹ A recently declassified 2020 National Intelligence Council assessment reports that China and other authoritarian regimes continue to use improved cyber capabilities and big data technologies to conduct large-scale espionage and micro-targeted influence campaigns against U.S. citizens.²³² A RAND report that analyzed Chinese military books, articles, and academic journals found that “the fundamental enabler of future Chinese psychological warfare information content is data—as much personal data as China can acquire, by any means necessary.”²³³ The same report states that machine-

²²⁷ JP 3-04, I-2–I-4.

²²⁸ Office of the Secretary of Defense, *Military and Security Developments Involving the PRC* (Washington, DC: Department of Defense, November 29, 2022). <http://defense.gov/CMPR>

²²⁹ Broadly defined as the employment of all the means at a nation’s command, short of war, to achieve its national objectives. For a thorough review of the terms and definitions needed to understand PRC political warfare and a historical overview of the PRC’s development of its political warfare capabilities, see Kerry Gershaneck, *To Win without Fighting: Defining China’s Political Warfare* (Quantico, VA: Marine Corps University Press, 2020). <https://doi.org/10.36304/ExpwMCUP.2020.04>.

²³⁰ Shinji Yamaguchi, Masaaki Yatsuzuka, and Rira Momma, “China’s Quest for Control of the Cognitive Domain and Gray Zone Situations,” *China Security Report 2023* (Tokyo, Japan: National Institute for Defense Studies Japan, 2022). <http://www.nids.mod.go.jp/english/publication/chinareport/index.html>.

²³¹ DoD Report to Congress, Network Centric Warfare, section. 3-9, 27 Jul 2001, http://www.dodccrp.org/files/new_report/report/new_main.pdf.

²³² NIC Assessment, “Cyber Operations Enabling Expansive Digital Authoritarianism, NICA 2020-027, 7 Apr 2020. <https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Cyber-Operations-Enabling-Expansive-Digital-Authoritarianism-20200407-2022.pdf>.

²³³ Nathan Beauchamp-Mustafaga, *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States* (RAND Corporation, June 20, 2023). https://www.rand.org/pubs/research_reports/RRA853-1.html.

manipulated information (e.g., deepfakes) “can be used to impersonate military personnel, spread rumors to confuse people or undermine military morale, and incite public anger to cause mass incidents.”²³⁴ The powerful role of emerging technology and AI-driven data analytics against the growing volume of commercially available personal data will only continue to increase this threat.

The DoD identified the PRC as “the pacing threat for the United States,”²³⁵ and it is clear that CCP leadership is resolute in using any and all means available to prevail in this decisive decade of strategic competition. The PRC whole-of-government approach to coerce other countries and undermine norms established by the international community involves cyberspace operations against the U.S. homeland and its citizens, overt/covert influence campaigns focused on shaping U.S. perceptions toward China, and operations that further stress the social and cultural divides between population groups in the United States.²³⁶ While possibly limited in scope and overall influence, the astounding popularity of the social media app TikTok (more than 150 million U.S. users as of March 2023) has U.S. policymakers concerned that the app’s algorithm could be “artificially promoting and/or suppressing certain content, perhaps leveraging the apps’ capability to microtarget specific audiences.”²³⁷ But the CCP’s more overt global media influence efforts reach a far greater number of people around the world, particularly audiences in the Global South. Freedom House’s September 2022 study (see Figure 7-1.) found that, in addition to the Chinese government expanding its global media footprint over the past three years, the CCP and its proxies have resorted to “harassment and intimidation of outlets that publish news or opinions disfavored by the Chinese government, and the use of cyberbullying, fake social media accounts, and targeted disinformation campaigns.”²³⁸

²³⁴ Ibid.

²³⁵ J. Garamone, “New Strategy Seeks to Reinvigorate Deterrence in a Changing World,” *DOD News*, November 7, 2022. <https://www.defense.gov/News/News-Stories/Article/Article/3212005/new-strategy-seeks-to-reinvigorate-deterrence-in-a-changing-world/#:~:text=China%20is%20the%20pacing%20threat,is%20fundamentally%20changing%2C%20Kahl%20said.>

²³⁶ Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, February 6, Feb 2023. <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2023/item/2363-2023-annual-threat-assessment-of-the-u-s-intelligence-community>.

²³⁷ Jon Bateman, *U.S.-China Technological “Decoupling”: A Strategy and Policy Framework* (Carnegie Endowment for International Peace, April 25, 2022). <https://carnegieendowment.org/2022/04/25/limiting-chinese-influence-operations-pub-86923>.

²³⁸ Sarah Cook, Angeli Datt, Ellie Young, and BC Han, *Beijing’s Global Media Influence* (Freedom House, September 2022). <https://freedomhouse.org/report/beijing-global-media-influence/2022/authoritarian-expansion-power-democratic-resilience>.

UNCLASSIFIED

Beijing's Tactics for Global Media Influence

The Chinese Communist Party (CCP) and its proxies influence news and information flows around the world through a range of activities. These were the most notable tactics observed in the 30 countries under study from 2019 to 2021.

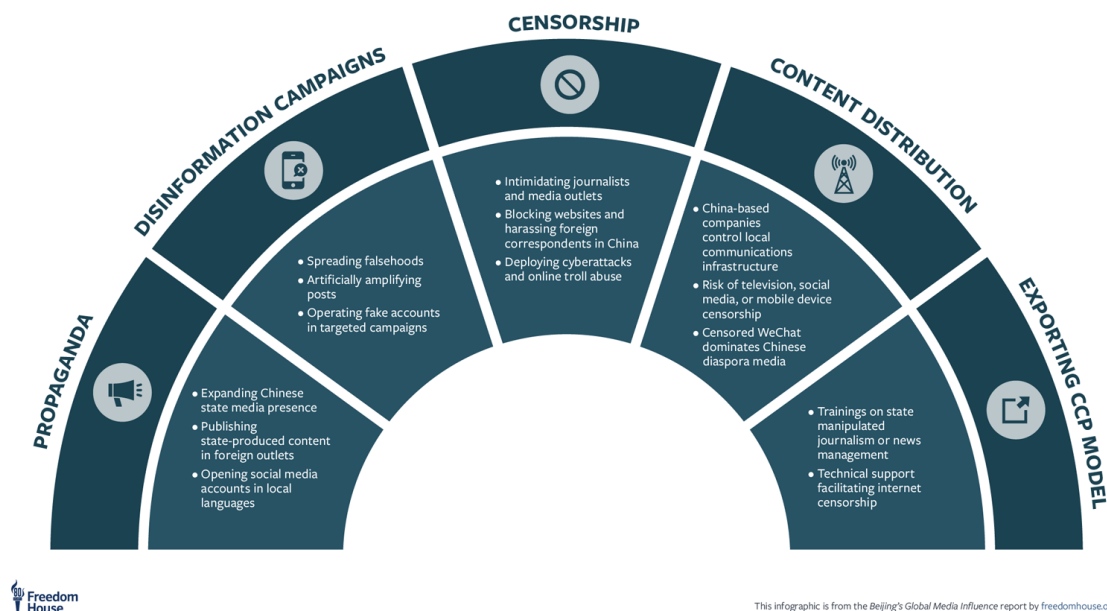


Figure 7-1. Beijing's Tactics for Global Media Influence²³⁹

C. The Russian Federation

Another major threat in the information domain is Russia's exploitation and influence efforts against liberal democratic societies.²⁴⁰ Though Russia and its intelligence services primarily utilize OIE as a method of information control for its own population, they also conduct aggressive OIE against adversaries through cyberspace.²⁴¹ With the steady progress of Internet technology, Russia's military intelligence unit (GRU) continuously develops and refines its capabilities to conduct cyberespionage and disinformation activities.²⁴² Russia has repeatedly conducted

²³⁹ Ibid.

²⁴⁰ For a thorough record of Russian Intelligence misinformation and influence operations, see Chapter 7 of Kevin P. Riehle, *Russian Intelligence: A Case-based Study of Russian Services and Missions Past and Present* (National Intelligence University, Spring 2022). https://ni-u.edu/wp/wp-content/uploads/2022/05/Riehle_Russian-Intelligence.pdf.

²⁴¹ Lev Topor and Alexander Tabachnik, "Russian Cyber Information Warfare: International Distribution and Domestic Control," *Journal of Advanced Military Studies* 12, no.1 (Spring 2021). <https://doi.org/10.21140/mcu.20211201005>.

²⁴² Andrew S. Bowen, *Russian Military Intelligence: Background and Issues for Congress* (Congressional Research Service, November 15, 2021). <https://crsreports.congress.gov/product/pdf/R/R46616/7>.

activities meant to spread falsehoods, influence behaviors, and justify armed conflict via false-flag operations.²⁴³ Russia's operations range from propaganda—which is characteristically high-volume and multi-channel; rapid, continuous, and repetitive; lacking commitment to objective reality; and lacking commitment to consistency—to the framing concept of reflexive control, which uses “psychological effects on decision-makers, communicates false or partially false information, coerces the enemy to envision defeat, and uses the enemy's resources against it,”^{244,245} Russia has no qualms with using any means necessary to wage their war on facts.

Russia's influence campaign against the 2016 U.S. presidential election highlighted the fissures within and fragility of American democratic society.²⁴⁶ In addition to the email hacks against the Democratic National Convention, stories of Russian troll factories funding and organizing protests and counter-protests during the election period fed the flames of uncertainty regarding the true extent of Putin's IW capabilities.^{247,248} While there was no evidence of changed votes or manipulated vote tallies, and a study on Russian interference found no real consequence on the final outcome of the election, Russia's efforts still inflicted a great deal of damage.^{249,250} Mistrust in the U.S. government and in the ability of big tech companies to protect information and the truth had taken hold in the American psyche.²⁵¹

²⁴³ Global Engagement Center, *Disinformation Roulette: The Kremlin's Year of Lies to Justify an Unjustifiable War*, U.S. Department of State, February 23, 2023. <https://www.state.gov/disarming-disinformation/disinformation-roulette-the-kremlins-year-of-lies-to-justify-an-unjustifiable-war/>.

²⁴⁴ Christopher Paul and Miriam Matthews, “The Russian “Firehose of Falsehood” Propaganda Model, RAND Corporation, 2016. <https://www.rand.org/pubs/perspectives/PE198.html>.

²⁴⁵ Samantha Mullaney, “Everything Flows: Russian Information Warfare Forms and Tactics in Ukraine and the US Between 2014 and 2020,” *The Cyber Defense Review* 7, no. 4 (Fall 2022). https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/12_Mullaney.pdf.

²⁴⁶ Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

²⁴⁷ Shaun Walker, “Russian Troll Factory Paid US Activists to Help Fund Protests During Election,” *The Guardian*, October 17, 2017. <https://www.theguardian.com/world/2017/oct/17/russian-troll-factory-activists-protests-us-election>.

²⁴⁸ Ryan Lucas, “How Russia Used Facebook To Organize 2 Sets of Protesters,” National Public Radio, November 1, 2017. <https://www.npr.org/2017/11/01/561427876/how-russia-used-facebook-to-organize-two-sets-of-protesters>.

²⁴⁹ U.S. Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Elections*, 116th Congress 1st Session, Report 116-XX, August 2020. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

²⁵⁰ Gregory Eady, Tom Paskhalis, Jan Zilinsky et al., “Exposure to the Russian Internet Research Agency Foreign Influence Campaign on Twitter in the 2016 US Election and Its Relationship to Attitudes and Voting Behavior,” *Nature Communications* 14, Article # 62, January 9, 2023. <https://doi.org/10.1038/s41467-022-35576-9>.

²⁵¹ Michael Barthel, Amy Mitchell, and Jesse Holcomb, “Many Americans Believe Fake News Is Sowing Confusion,” Pew Research Center, December 15, 2016. <https://www.pewresearch.org/journalism/2016/12/15/many-americans-believe-fake-news-is-sowing-confusion/>.

Russia's onslaught against the U.S. and its allies continues to this day. Russia is now considered one of the most serious foreign influence threats to the U.S. based on its use of intelligence services, proxies, and wide-ranging influence tools to try to divide Western alliances and increase its sway around the world while attempting to undermine U.S. global standing, sow discord inside the U.S., and influence U.S. voters and decision making.²⁵²

D. Islamic Republic of Iran and Democratic People's Republic of Korea (DPRK)

Other state actors that pose threats to the U.S. include Iran and the Democratic People's Republic of Korea (DPRK). As they cannot compete militarily against the United States, the majority of their OIE focuses on regime stability and regional influence operations. Iran uses strategic communication to counter U.S. narratives while promulgating their own and focuses its diplomacy efforts to support regional interests that meet its objectives.²⁵³ The Islamic Revolutionary Guard Corps (IRGC) is instrumental to furthering Iran's influence beyond its borders via participation in various global institutions.²⁵⁴ The Commander of U.S. Central Command (USCENTCOM) noted that the regime invests heavily in information operations, including broadcasting, coordinated inauthentic activity, and cyberattacks. The regime also supports violent proxy groups that spread chaos and instability throughout the region, and often aligns its information operations with or in support of Russia.²⁵⁵

Similar to Iran, the DPRK uses the cyberspace domain to conduct deniable, low-cost, low-risk influence, espionage, and criminal activities, and a threat of cyberattack against U.S. business and infrastructure remains a looming possibility.²⁵⁶ According to Admiral Aquilino, Commander USINDOPACOM, the DRPK "uses cyber programs to steal intellectual property and generate revenue, which includes the theft of crypto assets that helps finance weapons research and development."²⁵⁷ There are also two organizations in the Korean Workers' Party responsible for more traditional IW efforts. The United Front Department pushes overt propaganda and the

²⁵² ODNI, *Annual Threat Assessment of the U.S. Intelligence Community*, February 2023.

²⁵³ Itay Haiminis, "Iran's Information Warfare," in *The Cognitive Campaign: Strategic and Intelligence Perspectives*, ed. Yossi Kuperwasser and David Siman-Tov (Institute for National Security Studies and The Institute for the Research of the Methodology of Intelligence, 2019, 135–135147). https://www.terrorism-info.org.il/app/uploads/2019/11/H_259_19.pdf.

²⁵⁴ Mark Silinsky, *Iran's IRGC: Its Foreign Policy and Foreign Legion* (Quantico, VA: Marine Corps University Press, September 16, 2019). <https://doi.org/10.36304/ExpwMCUP.2019.01>.

²⁵⁵ Gen. Michael Kurilla, USA, "Statement on the Posture of USCENTCOM - SASC Hearing," March 16, 2023. <https://www.centcom.mil/ABOUT-US/POSTURE-STATEMENT/>.

²⁵⁶ ODNI, *Annual Threat Assessment of the U.S. Intelligence Community*, February 2023.

²⁵⁷ Adm. John Aquilino, USN, "HASC Opening Remarks on USINDOPACOM Posture," April 18, 2023. <https://www.pacom.mil/Media/Speeches-Testimony/Article/3369315/house-armed-services-committee-hasc-opening-remarks-april-2023/>.

creation of pro-North Korean groups within South Korea, while the Cultural Exchange Bureau (CEB) clandestinely uses agents to “establish underground political parties focused on fomenting unrest, revolution, or pro-DPRK views. The CEB also conducts clandestine influence operations.”²⁵⁸ Both of these state actors will continue to threaten U.S. posture and service members with their malign OIE.

E. Islamic State of Iraq and al-Sham (ISIS)

Non-state actors may not have the same resources to perform overarching influence campaigns against the U.S. Armed Services, but limited OIE effects can still have a global impact. Website defacements, data leaks, and propaganda can still create confusion and fear. In 2015, supporters of the Islamic State hacked multiple military social media accounts, posting messages and videos meant to frighten service members and civilians working at USCENTCOM.²⁵⁹ While the actual threat to forces was minimal and no military networks were compromised, the appearance of being vulnerable to the adversary can affect morale and induce fear in service members and their families. David Lapan (Col., USMC, Ret.) described an incident when unconfirmed reports claimed that eight Marines had been captured by a terrorist organization at the Iraq-Syria border. Due to bureaucratic miscommunication, it took U.S. forces eight hours to verify that that this had been a false report. Lapan stated, “How many potential recruits did the terrorist organization get over that period of time where it looked like they had the upper hand over U.S. Marines? How many ... were further intimidated ... that a terrorist organization had the upper hand?”²⁶⁰

ISIS also disseminates graphic depictions of beheadings and executions, creating a nightmarish virtual landscape meant to recruit new members with a taste for violence and to encourage malicious actors.²⁶¹

F. Threat Overview

This rest of this section reviews the IC’s process for prioritizing collection, analysis, and production and also offers an unclassified summary of the cyberexploitation threat based on the

²⁵⁸ Defense Intelligence Agency, *North Korea Military Power: A Growing Regional and Global Threat*, October 15, 2021. <https://www.dia.mil/Portals/110/Documents/News/NKMP.pdf>.

²⁵⁹ Dan Lamothe, “U.S. Military Social Media Accounts Apparently Hacked,” *The Washington Post*, January 12, 2015. <https://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-state-sympathizers/>.

²⁶⁰ Hayley Britzky, “The US Military Is Still Struggling to Figure Out Social Media,” *Task & Purpose*, November 2, 2022. <https://taskandpurpose.com/news/military-social-media-challenges/>.

²⁶¹ Catherine Theohary, “Information Warfare: Issues for Congress,” Congressional Research Service, March 5, 2018. <https://crsreports.congress.gov/product/pdf/R/R45142/5>.

most recent Intelligence Community (IC) Statements for the Record and other official sources. Additional detail on the threat is included in the classified annex to this report.

G. How U.S. Intelligence Agencies Prioritize Cyberexploitation

JP 3-04 defines the concept of the information environment (IE), which gives context to how the IC treats cyberexploitation: “[The IE is] the aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information.”²⁶²

Translating the IE to the terms defined in section 589F of the 2021 NDAA, cyberexploitation encompasses a range of activities founded in malign intent from an adversary intent on reducing or influencing U.S. national security priorities.²⁶³ Regardless of how cyberexploitation is defined, the negative outcome is well documented, and intelligence agencies have begun to adapt to the threat since the Russian election interference in 2016 and the January 6th insurrection. In 2017, Clint Watts, a senior fellow with George Washington University Center for Cyber and Homeland Security, stated that “it was social media that made Russia’s information operations so effective and efficient [in the 2016 election], particularly social media-enabled social engineering, identity theft, targeted advertisements, profiling through psychometrics, dissemination through bots, trending algorithms, creation of false personas, and psychological hacks to increase trust and verisimilitude. The psychology behind pleasure, rewards, social groups, and fear makes social media addictive and credible. This is the same psychology that makes social media’s use in information operations so pernicious and possibly impossible to counter.”²⁶⁴ It also makes traditional intelligence and counterintelligence (CI) operations effective and extremely difficult to detect and defeat.

The National Intelligence Priorities Framework (NIPF) is designed to maximize available resources to address a wide range of topics central to national security. While the specifics are classified, Intelligence Community Directive (ICD) 204 states that “The NIPF provides the mechanism for the development and communication of overarching national intelligence priorities and the evaluation of IC responsiveness and progress against those priorities.”²⁶⁵ The framework also provides a process for ad hoc updates to national intelligence priorities, which is driven by

²⁶² JP 3-04, Information in Joint Operations, September 14, 2022, <https://pavilion.dinfos.edu/Portals/1/Documents/JP%203-04%20Information%20in%20Joint%20Operations.pdf>.

²⁶³ 2021 NDAA §589F

²⁶⁴ G. Jakubowski, “What’s Not to Like? Social Media as Information Operations Force Multiplier,” *Joint Forces Quarterly*, July 1, 2019. <https://ndupress.ndu.edu>.

²⁶⁵ ICD 204, National Intelligence Priorities Framework, https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf.

the need to generate greater targeting, collection, processing, exploitation analysis, and dissemination of intelligence on any topic, especially across-the-seam issues like cyberexploitation.

The need to update the NIPF has gained visibility outside of government. In 2022, the Atlantic Council recommended that the NIPF include requirements that drive further understanding of how adversaries manipulate and weaponize information, as well as the potential political and social ramifications. The Atlantic Council also recommended expanding the ability to suggest changes to NIPF priorities to organizations collecting open-source intelligence (OSINT), as foreign influence operations often occur in the public domain.²⁶⁶

H. Office of the Director of National Intelligence (ODNI)

While the Office of the Director of National Intelligence (ODNI) is not directly responsible for sharing analysis and education on cyberexploitation and online deception threats with service members and their families, related topics feature prominently in unclassified ODNI testimony and public-facing media. In 2023, Director of National Intelligence (DNI) Avril Haines' public testimony made frequent and wide-ranging comment on the risks of foreign malign cyberexploitation, including the use of social media. The DNI reported that foreign states' malicious use of digital information and communication technologies will become more pervasive, automated, targeted, and complex during the next few years, further threatening to distort publicly available information and likely outpacing efforts to protect digital freedoms. The exploitation of U.S. citizens' sensitive data and illegitimate use of technology, including commercial spyware and surveillance technology, will likely continue to threaten U.S. interests.²⁶⁷

The ODNI Annual Report takes direct aim at China's capability and intent in this area, especially prior to any commencement of hostilities, and while not calling out the risk to U.S. service members directly, the inference is clear:

If Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure and military assets worldwide. Such a strike would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces...China leads the world in applying surveillance and censorship to monitor its population and repress dissent. Beijing conducts cyber intrusions that are targeted to affect

²⁶⁶ J. Counter, "How the US Can Focus Its Fight Against Foreign Influence Operations" *Atlantic Council*, September 30, 2022. <https://www.atlanticcouncil.org/content-series/hybrid-warfare-project/how-the-us-can-focus-its-fight-against-foreign-influence-operations/>.

²⁶⁷ Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, 27.

U.S. and non-U.S. citizens beyond its borders—including journalists, dissidents, and individuals it views as threats.

The Foreign Malign Influence Center (FMIC) was established under the auspices of ODNI in September 2022 to “counter enduring threats to democracy and U.S. national interests from foreign malign influence (FMI) actors by integrating analysis, managing the intelligence mission, nurturing partnerships, and providing indications and warning of foreign malign influence.”²⁶⁸ While this mission does not overlap wholly with cyberexploitation and deception of U.S. service members, the Center could play an important role in facilitating interagency collaboration and producing policy-informative insights for the DoD.

I. Defense Intelligence Agency (DIA)

As early as 2021, the DIA Director highlighted the risk of cyberexploitation and online deception of service members from an operational perspective, stating:

Adversarial malicious cyber operations are also increasingly difficult to observe and attribute. We are particularly concerned with adversaries probing and exploiting our military and intelligence networks, *sustained targeting of military social media to manipulate our personnel and monitor movement of U.S. forces*, and attempts to compromise the U.S. defense-industrial base in order to steal weapons systems technology.²⁶⁹

The DIA Director repeated this message in 2022, adding the concern that Russia will “probably use artificial intelligence to develop autonomous cyber capabilities to optimize offensive cyberoperations and automate social media operations designed to exacerbate social divides.”²⁷⁰

1. Defense Intelligence Agency (DIA) Innovation Outreach Through NeedipeDIA

DIA uses NeedipeDIA, an unclassified site, to engage with academia and industry to highlight areas for collaboration and innovation, and details those areas where management is open to outreach from industry. As of June 2023, two of the items on the site’s current needs list, Enhance Counterintelligence and Security and AI/ML Support to Cybersecurity (see Figure 7-2), are related to cyberexploitation and online deception.²⁷¹

1.18 AI & ML Support to Cybersecurity: DIA seeks to improve capabilities for applying artificial intelligence and machine learning to the target area of cybersecurity. Solution would have the ability to dynamically detect anomalies/risks/threats and then to alert defenders. The capability must be able to perform these functions at a greater scale and pace than what is currently accomplished using the traditional collect, process, and analyze methodology.

²⁶⁸ The Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020, Pub. L. 116-92, 50 U.S.C. §3059.

²⁶⁹ LTG Scott Berrier, U.S. Army; “Statement for the Record: Worldwide Threat Assessment – 2021.”

²⁷⁰ LTG Scott Berrier, U.S. Army, “Statement for the Record: Worldwide Threat Assessment – 2022.”

²⁷¹ <https://www.dia.mil/Business/NeedipeDia/>.

Figure 7-2. DIA Need/DIA Related to Cyberexploitation

J. National Security Agency

The National Security Agency (NSA) has a decades-long history of engaging with the private sector on cybersecurity best practices. The NSA has issued relevant press releases and maintained a public facing set of resources on www.nsa.gov, featuring information sheets, advisories and technical reports related to cybersecurity.²⁷² While many of these documents take a highly technical approach aimed at supporting DoD services, contractors, industry and the general public, some are focused on social media and home networking (see Figure 7-3).

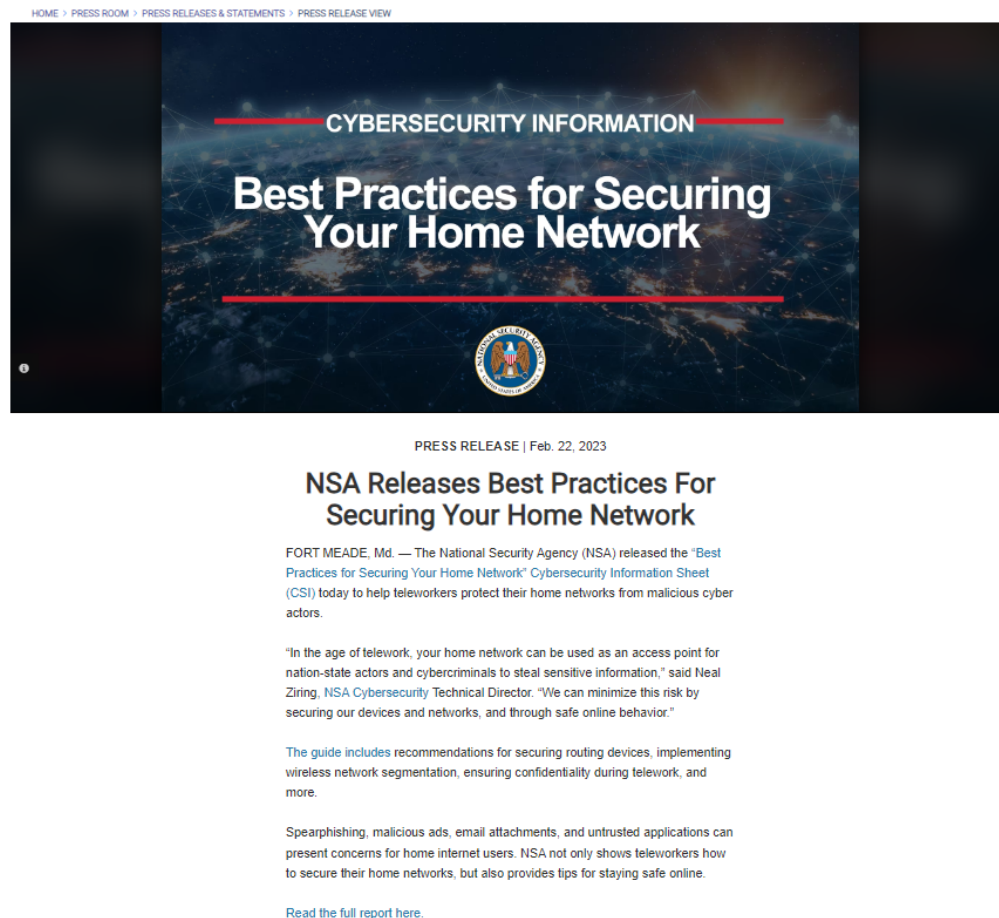


Figure 7-3. NSA's Best Practices for Securing Home Networks

²⁷² National Security Agency, "NSA Cybersecurity Advisories and Guidance." <https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/>.

8. DoD Education and Training

This section examines DoD's efforts to educate and inform service members and their families about what they can do to safeguard their information online and reduce the risk of cyberexploitation.

A. DoD Actions to Reduce the Unauthorized Access of Personal Information for Malicious Purposes

In March 2021, the DoD released an Identity Awareness, Protection, and Management Guide to educate service members on how to protect their privacy and identity online, including recommendations and best practices for online platforms (e.g., Facebook, Instagram, LinkedIn, TikTok, Twitter, Google), mobile applications, and devices such as cell phones and fitness trackers.²⁷³ The guide provides instructions for opting out of data aggregators that vacuum up personal information to sell. It also provides a guide for keeping kids safe online, which includes instructions for filtering sites to reduce exposure to cyber-bullying or influence operations and a discussion of services to restrict and monitor the content a child could see.²⁷⁴

B. Military Service Actions to Reduce Cyberexploitation through Education

In March 2021 testimony to the House Committee on Armed Services, Acting Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, Christopher Maier, highlighted the importance of counter-propaganda and force protection efforts for combatting misinformation, disinformation, and propaganda. He suggested that the DoD Office of Public Affairs release counter-propaganda campaigns to inform service members about propaganda techniques adversaries may use to target them for exploitation. He also stated that the responsibility for force protection lies with the Services, specifically educating service members on media literacy and helping them develop the critical thinking skills necessary to protect against misinformation.

The Services currently offer a number of guides and educational tools focusing on misinformation/disinformation and the unauthorized access of personal information online. The Army offers guides for official Army social media accounts and personal accounts. The official account guide includes guidance on passwords, acceptable conduct, and what to do if an account

²⁷³ https://www.odni.gov/files/NCSC/documents/campaign/DoD_IAPM_Guide_March_2021.pdf.

²⁷⁴ Ibid.

is hacked.²⁷⁵ The personal account guide delineates the differences between official and personal social media use and includes links to relevant training courses and a site capturing social media best practices.²⁷⁶

The Navy's *Social Media Handbook for Sailors & Families 2023* provides considerations for online behavior and stresses that sailors are subject to Navy and the Uniform Code of Military Justice (UCMJ) regulations even when they are off duty and posting on their personal social media accounts. The handbook also offers some information on media literacy and encourages sailors to "take the time to critically think about the information, consider its source, and any agenda of the source."²⁷⁷

The Air Force Public Affairs office published its *Social Media Guide* in 2021 for both official and personal social media accounts. The guide offers best practices for social media and warns service members that the material they post online, as adversaries may use that information to "impersonate, blackmail or intimidate."²⁷⁸ The guide specifies that service members should avoid sharing information about travel, location, deployment, or family members. The guide also provides official accounts with guidelines for handling incorrect social media posts, encouraging account administrators to acknowledge the mistake and post the correct information, if applicable.²⁷⁹

The Marine Corps' 2021 *Social Media Handbook* addresses military families directly, to inform them of the risks related to sharing personal information. But the guide also encourages military family members to join support networks on social media, including spouse's clubs and child care groups. The goal is a balanced approach to personal social media use, taking advantage of the opportunities it provides for connection while carefully and selectively posting information.²⁸⁰

C. The DoD Cyber Crime Center (DC3)

The DoD Cyber Crime Center (DC3) is responsible for establishing and maintaining high standards for digital and multimedia forensics in the DoD. It works with other DoD components to ensure that those standards are consistent and that the standards are effective.²⁸¹ It is also DoD policy that DC3 "develop and provide cyber investigative training for DoD and non-DoD

²⁷⁵ <https://www.army.mil/socialmedia/operations/index.html>.

²⁷⁶ <https://www.army.mil/socialmedia/>.

²⁷⁷ [https://media.defense.gov/2023/Mar/02/2003171513/-1/-1/0/SMP_SAILORSFAMILIES_V12%20\(1\).PDF](https://media.defense.gov/2023/Mar/02/2003171513/-1/-1/0/SMP_SAILORSFAMILIES_V12%20(1).PDF).

²⁷⁸ https://www.af.mil/Portals/1/documents/2021SAF/07_July/DAF_SM_Guide_Publication_v4.3.pdf.

²⁷⁹ Ibid.

²⁸⁰ <https://www.marines.mil/Portals/1/Docs/2021USMCSocialMediaHanbook.pdf>.

²⁸¹ <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/550513Ep.pdf>.

personnel, as authorized.”²⁸² This spurred DC3 to establish a Cyber Training Academy, which has the mission to “design, develop, and deliver the highest possible quality in cyber training to Department of Defense (DoD) personnel.”²⁸³ CTA’s Cyber Learning Management Environment (CLME) offers education and training modules on cyber risks, as well as webinars on pertinent topics. The Cyber Fundamentals 100 course offers “the first installment of a two-part curriculum providing foundational cyber knowledge to Defense Criminal Investigative Organizations’ (DCIOs) cyberspace workforce elements and Department of Defense (DOD) personnel, whose duties include protecting DOD information systems from unauthorized and/or illegal access.”²⁸⁴ The knowledge gained through this course could help service members reduce the risk of cyberexploitation and become more vigilant online. The follow-on course, Cyber Fundamentals 200, helps service members “determine the best cybersecurity defense practices to meet common security standards.”²⁸⁵

Though the CLME is open to service members, this training opportunity is not linked to enlistment. Making that connection would expose more service members to the training offered, which would improve cyber hygiene across the department. DoD policy states that non-DoD personnel can take this training, which opens up an avenue for service members’ families to learn as well.

D. DoD Privacy, Civil Liberties, and Freedom of Information Directorate (DPCLD) Partnership with the National Counterintelligence and Security Center (NCSC)

The DoD Privacy, Civil Liberties, and Freedom of Information Directorate (DPCLD) has collaborated with the National Counterintelligence and Security Center (NCSC) on multiple identity theft resources, some especially pertaining to reducing cyberexploitation risks.²⁸⁶

One document, “Protecting Your Personal Information from Exploitation,” provides guidance on safeguarding personal information. The document stresses the risks of sharing personal, financial, or other sensitive information online, and warns against sharing such information if contacted by unknown or individual groups. It provides insight into the various methods an adversary might use to harm a service member, improving their ability to anticipate

²⁸² DoD CIO, DoD Directive 5505.13E, DoD Executive Agent.

²⁸³ https://www.dc3.mil/Portals/100/Documents/DC3/Products/Factsheets/CTA/DC3-CTA-FactSheet-4JAN2023.pdf?ver=G4T_XgMN4MifSjNMEoRPAQ%3d%3d×tamp=1673445943826.

²⁸⁴ https://www.dc3.mil/Portals/100/Documents/DC3/Missions/CTA/Course%20Catalog/FY22/FY22%20Course%20Catalog.pdf?ver=rsJ_udwmcheSa0_xTbX-BA%3D%3D×tamp=1632142027379.

²⁸⁵ Ibid.

²⁸⁶ <https://dpclد.defense.gov/Privacy/Resources.aspx>.

and prevent risks and threats. The document also encourages service members to remain vigilant online and share the information with their families and friends.²⁸⁷

²⁸⁷ <https://dpcl.d.defense.gov/Privacy/Resources.aspx>.

9. Conclusions and Recommendations

The IDA team found minimal written policy, strategy, instruction, or regulation within the DoD assigning specific responsibilities to prevent the cyberexploitation or online deception of members of the Armed Forces or their families. The IDA team was also unable to find any one source of empirical data that could support a conclusion that members of the Armed Forces and/or their family members are targeted at a higher rate in comparison with the general population. However, insights gained through the extensive interview process with representatives of 20 organizations across the Office of the Secretary of Defense, the Military Services, the Combatant Commands, the Joint Staff, federal agencies, academia, and industry indicate that this may be a growing area of concern for the department.

It Is a “Seam” Issue. While cyberexploitation and online deception can be considered methods for enabling operations within the information domain, the methods are not typically executed through attacks on our networks, so it is not specifically a U.S. Cyber Command defensive responsibility. Much of the cyberexploitation and online deception activity are low-level scams aimed at stealing money from unsuspecting victims. Thus, this is also not a counterintelligence and insider threat mission.

The U.S. Military and Veteran Communities Are a Reflection of a Societal Issue. There is no meaningful way to opt out of commercial data collection, and this issue is not limited to the U.S. military and veteran communities, rather it represents a vulnerability for the whole of society. Everyday life requires each of us to partake in the services of online applications, shop online, use a smartphone, and connect with others through social media, making us vulnerable to having our personal data harvested, aggregated, curated and sold within the commercial data broker ecosystem. Government data at the federal, state and local levels, such as property records, driver license and driving records, voter registration records, and many other forms of government records are also available to be scraped or purchased. With the exception of a few states that have instantiated data privacy laws, there is no meaningful way to opt out of this data environment. The personal data about each of us is marketed and sold to companies who wish to sell us their products and services. Because of the volume of data that is collected, it is quite easy for commercial entities to target us with very personalized advertisements. In addition to companies who wish to engage us for legitimate commercial purposes, this same data is available to criminals who want to target us for more nefarious purposes like online scams or to foreign actors who wish to engage in

disruptive information operations.²⁸⁸ However, the demographics of the US Military and veteran populations make these communities an easy target for manipulation and exploitation. The negative effects of cyberexploitation and online deception can have negative impacts on readiness and can diminish unit cohesion, morale, and mission/combat effectiveness.

Information Operations Are Enabled and Amplified Through Technology. The rapid expansion of AI technology, machine-manipulated data (and “deepfakes”) and commercially available information (CAI) domains (also known as “data brokers”) have expanded the ability to target individuals. In the not too distant past, it would have taken the resources of an adversarial nation state actor to do what someone now can do in a basement with very limited technical ability or computing resources. The CAI that is known and inferred about each of us is readily available for purchase and can be used for precise targeting of individuals or sub-populations for operations ranging from simple financial scams, to radicalization, to purposeful degrading of unit cohesion and morale, and for targeting individuals to commit espionage. The speed, scale, and capability of these technology and data tools are expanding exponentially, suggesting that the situation will get worse over time.

We Are Willing Consumers of the Enabling Technology. In most cases, we as consumers have enabled the data broker ecosystem by accepting the terms of service and end user license agreements (EULAs) for the social media and other commercial applications that we use on our smartphones and other Internet-enabled devices. Most consumers are unaware of the scope and magnitude of CAI that is available on each of us. The data that is used to target us for marketing, criminal activity, scams, extortion, disruption, radicalization, or espionage is not acquired illegally — it is typically purchased legally on the open market.

Balancing Security, Civil Liberties, Privacy, and Transparency. The risk to the DoD at the individual, unit, organization, or even sub-population level could be reduced by restricting individuals from using social media and similar apps on smartphones and disallowing them from participating in the digital marketplace. However, that would have a negative impact on the ability to attract and retain a highly qualified fighting force and would likely be challenged as imposing on an individual’s privacy, civil liberties, and freedom of speech.

Legislation, Regulation, and Policy Have Not Kept Pace with Technology. Legislative, regulatory, and policy solutions to cyberexploitation and online deception issues have not kept pace with the rapid expansion of the enabling technology and the adversary’s use of that technology to exploit our vulnerability to their advantage.

²⁸⁸ Sherman, Justin, Haley Barton, Brady Klein, and Anushka Srinivasan. “Data Brokers and the Sale of Data on U.S. Military Personnel: Risks to Privacy, Safety, and National Security.” Duke University Sanford School of Public Policy. <https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/>.

A. Recommendations for Addressing Specific Avenues of Cyberexploitation

1. Predatory Financial Practices

Though the Department has no indication that service members and their families lack adequate access to necessary, responsible credit, predatory financial products are an issue.²⁸⁹ In fact, it is possible that service members underreport the use of high-cost, short-term financial products, as they are probably reluctant to truthfully answer questions regarding financial difficulties, given the potential consequences.

The MLA and financial literacy education, training, and resources have helped reduce service members' use of predatory financial products, as well as targeting attempts by organizations offering such products. In addition, the closure of the 90/10 loophole this year (2023) will directly address and reduce the aggressive and deceptive practices of some for-profit schools. However, the training and education that DoD provides must be continually updated to reflect the latest products and targeting techniques. This training must also focus on junior personnel, as they are the most susceptible. Financial literacy education should be introduced as early as possible—perhaps even in high schools—to provide a firm foundation for future service members. Financial literacy could also be included through courses in Junior Reserve Officer Training Corps (JROTC), Senior Reserve Officer Training Corps (SROTC), or other recruiter outreach and intake programs (e.g., Delayed Entry Program).²⁹⁰

2. Unproven and Unnecessary Medical Treatments

The medical market is always evolving, with new treatments and procedures constantly emerging. Although many of these new approaches will yield value for patients, there will inevitably be other treatments and procedures that remain unproven, unnecessary, and even dangerous. As long as people face challenging medical conditions without clear-cut treatments or seek easy solutions to common health issues such as weight loss, there will be a risk of individuals falling prey to unproven or unnecessary medical treatments or procedures. Though it does not seem that service members and their families are directly targeted in most cases, they are still vulnerable to these schemes.

DoD can best address this by providing media literacy training to educate service members on dubious medical claims and ways to spot them. DoD should also provide service members with information to help determine which products are sound and which are not, such as links to relevant FDA resources or other pertinent information.

²⁸⁹ Report on the Military Lending Act and the Effects of High Interest Rates on Readiness, Response to House Report 116-442, Title V, May 2021, p. 7, 121.

²⁹⁰ Congressional Research Service Report R46983, *Military Families and Financial Readiness*, January 12, 2022, 19.

3. Extremist and Racist Messaging

Approaches for countering violent extremism need to address the psychological, attitudinal (or emotional), and cognitive factors that allow individuals to adhere strongly to conspiracy theories, particularly those focused on political or societal grievances.²⁹¹ The effects of false information campaigns are not easily reversed, even when individuals acknowledge that their views are based on incorrect, false, or erroneous information, or if the information was openly labeled a conspiracy theory.²⁹² Further, government counter-messaging efforts may cause conspiracy theorists to double down on their beliefs regarding government corruption or secret government efforts to affect the public's cognition and behavior. Tactical responses, such as deployment of fact-checking tools or adjusted social media algorithms to disincentivize false information and prevent it from appearing on newsfeeds, have shown mixed efficacy. Instead, DoD should explore a multi-faceted approach to protect service members and their families from cyberexploitation by extremist groups and conspiracy theorists. Combining standardized social media screening for service members with digital and media literacy training and education would reinforce critical thinking skills both online and offline to help service members and their families identify extremist and conspiracy theory messaging and disrupt its spread.

An inoculation approach uses media literacy education as a means of generating immunity against false information and/or malicious persuasion attempts. One method is to train readers to evaluate information for consistence, congruence, and coherence to compare new and previously known information and edit the text for accuracy. This editorial approach has been shown to decrease an individual's susceptibility to false information and decreases the likelihood that they will share the false information online.²⁹³ Another method involves asking readers to explain why a statement is true or false, relying on the individual to decide on the accuracy of the statement and thus removing any debate regarding the arbiter of truth.²⁹⁴

²⁹¹ Ibid. For political issues, assessing what constitutes a false story and false information has an added layer of complexity, as many media outlets have political leanings and may be selective about what they cover, how much prominence it receives, and the context in which it is presented. The information in a news story may indeed be factual, but without providing an adequately broad and neutral context, the story may appear to be more of a half-truth or an editorial to someone holding opposing views. An assertion by a news organization with a known political leaning that a piece of information opposing their political view is "false information" may consequently be discounted or fall on deaf ears.

²⁹² K. M.-W. Douglas and R. M. Sutton, "Is the Label 'Conspiracy Theory' a Cause or a Consequence of Disbelief in Alternative Narratives?" *British Journal of Psychology* 113, no. 3 (2021): 1–16; J. Jerit and Y. Zhao, "Political Misinformation," 77–94.

²⁹³ Note that this editorial approach requires careful planning, as drawing a reader's attention to inaccurate information increases their exposure to false information, leading to negative results. L. Fazio, "Pausing to Consider why a Headline Is True or False Can Help Reduce the Sharing of False News," *The Harvard Kennedy School Misinformation Review* 1, no. (2 (2020):), 1–8; A. N. Eslick, L. K. Fazio, and E. J. Marsh, "Ironical Effects of Drawing Attention to Story Errors," *Memory* 19 (2011): 184–191.

²⁹⁴ Fazio (2020) conducted a study in which she engaged some participants in this very exercise. Prior to rating how likely they were to share a political news story based on the headline alone, she asked participants to explain

These inoculation approaches encourage readers to slow down and think more deeply about the information they consume.²⁹⁵ These prompts may also shift readers' motivations for sharing information, increasing the value of accurate information over information that is merely entertaining.²⁹⁶

The Services have minimum standards for digital literacy—the Air Force, for example, considers digital literacy to be a core competency²⁹⁷ and uses MyVector to deploy a digital literacy self-assessment for Airmen—but such standards are not consistent throughout the Department as a whole. The DoD should establish an overarching policy and standard to guide digital literacy requirements for all service members.

4. Sextortion

As a result of the Marines United scandal, the Marine Corps changed the Uniform Code of Military Justice (UCMJ) to criminalize the non-consensual sharing of nude photos. Though these changes have not eliminated the problem of online sexual harassment, they do provide an avenue for recourse. Expanding these prohibitions in the UCMJ to explicitly include the creation and distribution of deepfaked pornography will provide a similar avenue for recourse.

Generative AI's implications on the future evolution of sexual extortion should be included in any sextortion-related educational material created for service members. The FBI states that reducing the number of facial images available online for cybercriminals to use would have a risk-reduction effect. However, that advice is now out of date, as new apps enable the creation of realistic videos from a single photo. Servicewomen will likely be targeted with deepfake pornography, but they are not the only ones. Consider the perspective of a state-sponsored cybercriminal, aiming to undermine troop morale or distract senior leadership before a major military operation by their nation. They may conduct a targeted sextortion campaign of senior leadership or their families using deepfaked sexual videos. State-sponsored cybercriminals also may wish to harm unit cohesion by releasing deepfake pornography of servicewomen and using impersonation accounts to bolster circulation. Widespread targeting of servicewomen may create retention issues if the situations are not handled properly and the victims feel re-victimized by their coworkers.

how they determined whether the headline was true. This accuracy prompt led to a reduction in participants' intentions to share false headlines but had no effect on true headlines. This effect was largest when participants were seeing the headline for the first time.

²⁹⁵ B. Bago, D. G. Rand, and G. Pennycook, "Fake News, Fast and Slow: Deliberation Reduces Belief in False (But Not True) News Headlines," *Journal of Experimental Psychology: General* 149, no. 8 (2020), 1608–1613.

²⁹⁶ L. Fazio, "Pausing to Consider Why a Headline Is True or False Can Help Reduce the Sharing of False News," 1–8.

²⁹⁷ U.S. Department of the Air Force, *Foundational Competencies: Digital Literacy*, 2021.
<https://www.af.mil/News/Article-Display/Article/2773797/foundational-competencies-digital-literacy/>.

It is nearly impossible to prevent the creation of pornographic deepfakes, whether they victimize female military members or high-level leadership. DoD needs to provide service members with guidance for dealing with these issues if and when they occur. The guidelines should encourage service members to refuse to pay cybercriminals who threaten to release pornographic deepfakes, view explicit images of their coworkers with skepticism, and refrain from downloading or sharing such images or videos if they see them.

5. Cyberexploitation by Foreign Threats

Given the exponential growth of technology in the past two decades, cyberexploitation and online deception will be an ever-increasing threat to service members and their families. Conventional military operations will continue to adapt and find new, creative ways of complementing intelligence collection and kinetic operations with IW tactics, techniques, and procedures, but cyber “soft-targets” will always be lucrative objectives for online criminals and malicious actors. A thorough and persistent addition of proactive measures and countermeasures will be required to build, protect, and sustain the morale of service members and their families.

DoD should focus on conducting command information activities to establish reliable and secure communications, conducting counter-deception and counter-propaganda activities, verifying trustworthy sources of information, and facilitating face-to-face communication among command teams and service members to address this threat.²⁹⁸

B. Overall Recommendations

The IDA team makes the following recommendations.

Enact a Data Privacy and Protection Act. Adopt and enact a data privacy framework within the United States analogous to the General Data Protection Regulation (GDPR) that has been in place within the European Union since 2016. There is currently no comprehensive federal data privacy law in the United States, but there have been ongoing discussions in Congress regarding the American Data Privacy and Protection Act (ADPPA).

The American Data Privacy and Protection Act, H.R. 8152, would create a comprehensive federal consumer privacy framework. The ADPPA regulation is similar to the GDPR in its coverage of entities and personal data.

From the Congressional Research Service:

The bill would prohibit covered entities from collecting, using, or transferring covered data beyond what is reasonably necessary and proportionate to provide a service requested by the individual, unless the collection, use, or disclosure would fall under one of seventeen permissible purposes. It also would create special

²⁹⁸ JP 3-04, II-14.

protections for certain types of sensitive covered data, defined as sixteen different categories of data. Among other things, the bill would require covered entities to get a consumer's affirmative, express consent before transferring their sensitive covered data to a third party, unless a specific exception applies.²⁹⁹

The GDPR has been used as a model for the data privacy laws in Turkey, Mauritius, Chile, Japan, Brazil, South Korea, South Africa, Argentina, and Kenya. The UK retains the GDPR in identical form.

Enable a Meaningful and Comprehensive “Opt Out” Framework. Enact legislation that enables a meaningful “opt out” from the data broker ecosystem and allows members of the armed services and their families to “be digitally forgotten” by removing commercially available information from data broker database. Today there are limited means to opt out of the commercial data marketplace. And the methods that do exist are expensive, time consuming, and are legally vague about whether the companies will actually adhere to the opt out requests.

Expand Digital Persona Protection. Expand digital persona protection as detailed in DoDI O-2000.22 to include all DoD flag officers and senior executive personnel. The expanded DoDI O-2000.22 can also be supplemented by subsidizing a set of privacy enhancing services, tools and technologies to enable service members and families the opportunity to proactively manage their digital identity.

Assign Responsibility with Congruent Authorities. Establish a champion within the DoD to advocate for and enable the protection of digital identity management for members of the Armed Services and their families.

Potential Next Steps for DoD

Initiate Data Collection. Collect empirical data to demonstrate extent of the cyberexploitation of members of the Armed Services and their families.

Leverage the Joint Capabilities Integration and Development System (JCIDS). Establish a requirement to provide digital protections to US service members and their families. A formal JCIDS requirement for “All Domain Protection” would be instrumental for establishing services to assist members of the armed services in managing their digital identity and could minimize their exposure to the harmful effects of cyberexploitation and online deception. There is a capability-based assessment (CBA) by the U.S. Army’s Maneuver Center of Excellence that is developing a requirement for “all domain protection” that includes protections within the information domain.

Leverage Best Practices within DoD. Empower the special operations community to scale up a “cyber hygiene scorecard” that can be expanded to other sensitive mission areas or sub-

²⁹⁹ Congressional Research Service, Overview of the American Data Privacy & Protection Act, H.R.8152, Overview of the American Data Privacy and Protection Act, H.R. 8152 (congress.gov), August 31, 2022, p. 2.

populations, such as the IC, the nuclear command, control and communications (NC3) Community, and more.

Identity Management and Its Impacts on Readiness. Ensure that digital identity management and digital hygiene at the individual and unit level is considered in the new readiness framework being developed by the Assistant Secretary of Defense for Readiness.

Appendix A. Interviewees

Office of the Secretary of Defense

Department of Defense Insider Threat Management Analysis Center (DITMAC)

Department of Defense Office of Intelligence and Security (OUSD/I&S)

Department of Defense Office of Personnel and Readiness Defense Health Agency

Department of Defense Office of Public Affairs (OUSD/PA)

Defense Advanced Research Projects Agency, Information Innovation Office (DARPA/I2O)

Department of Health & Human Services (HHS)

Department of Homeland Security Office of Intelligence & Analysis (DHS/I&A)

Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS/CISA)

Department of Veterans Affairs (VA)

Joint Staff, J39

Joint Staff, J6

Joint Staff Security Office (JSSO)

Naval Criminal Investigative Service (NCIS)

Army Criminal Investigative Division (Army CID)

Air Force Office of Special Investigations (AFOSI)

Defense Cyber Crimes Center (DC3)

Army Cyber Institute (ACI)

Office of the Director of National Intelligence (ODNI)

Foreign Malign Influence Center (FMIC)

National Counterintelligence & Security Center (NCSC)

National Insider Threat Task Force (NITTF)

National Security Agency (NSA)

Defense Intelligence Agency, Defense Cover Office (DIA/DCO)

United States Indo-Pacific Command (Pacific Sentry)

United States Special Operations Command (USSOC)

United States Army Special Operations Command (USASOC)

United States Cyber Command (USCC)

Duke University

New York University

Graphika

Moonshot

Meta

Thomson Reuters Special Security

Appendix B. References

- Amarasingam, Amarnath. “The Impact of Conspiracy Theories and How to Counter Them: Reviewing the Literature on Conspiracy Theories and Radicalization to Violence.” In *Jihadist Terror: New Threats, New Responses*, edited by Anthony Richards, Devorah Margolin, and Nicolo Scremin, 27–40. London: IB Taurus, 2019.
- Amarasingam, Amarnath and Marc-André Argentino. “The QAnon Conspiracy Theory: A Security Threat in the Making?” *CTC Sentinel* 13, no. 7 (2020): 37–44.
- “Annual Threat Assessment of the U.S. Intelligence Community,” *Office of the Director of National Intelligence*, February 6, 2023, pg. 27, accessed June 20, 2023, <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf>, overall classification is UNCLASSIFIED.
- Anti-Defamation League. *Backgrounder: Patriot Front*. New York: Anti-Defamation League, 2022. <https://www.adl.org/resources/backgrounder/patriot-front>.
- Anti-Defamation League. *Funding Hate: How White Supremacists Raise Their Money*. New York: Anti-Defamation League, 2017. <https://www.adl.org/sites/default/files/adl-report-funding-hate-how-white-supremacists-raise-their-money.pdf>.
- Aquilino, John, Adm. U.S. Navy. “HASC Opening Remarks on USINDOPACOM Posture.” April 18, 2023. <https://www.pacom.mil/Media/Speeches-Testimony/Article/3369315/house-armed-services-committee-hasc-opening-remarks-april-2023/>.
- Bago, B., D. G. Rand, and G. Pennycook, “Fake News, Fast and Slow: Deliberation Reduces Belief in False (But Not True) News Headlines,” *Journal of Experimental Psychology: General* 149, no. 8 (2020): 1608–1613. doi:10.1037/xge0000729.
- Barthel, Michael, Amy Mitchell, and Jesse Holcomb. “Many Americans Believe Fake News Is Sowing Confusion.” Pew Research Center, December 15, 2016. <https://www.pewresearch.org/journalism/2016/12/15/many-americans-believe-fake-news-is-sowing-confusion/>.
- Bartlett, J., and C. Miller. *The Power of Unreason: Conspiracy Theories, Extremism and Counterterrorism*. London: Demos, 2010.
- Bartlett, Jamie, Jonathan Birdwell, and Michael King. *The Edge of Violence: A Radical Approach to Extremism*. London: Demos, 2010.
- Bateman, Jon. *U.S.-China Technological ‘Decoupling’: A Strategy and Policy Framework*. Carnegie Endowment for International Peace, April 25, 2022. <https://carnegieendowment.org/2022/04/25/limiting-chinese-influence-operations-pub-86923>.

- Beauchamp-Mustafaga, Nathan. *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States*. RAND Corporation, June 20, 2023. https://www.rand.org/pubs/research_reports/RRA853-1.html.
- Berrier, S., LTG U.S. Army, “Statement for the Record: Worldwide Threat Assessment – 2021.” April 29, 2021, accessed June 20, 2023, <https://www.dia.mil/Articles/Speeches-and-Testimonies/Article/2590462/statement-for-the-record-worldwide-threat-assessment-2021/>, overall classification is UNCLASSIFIED.
- Bhatt, S. and J. Mantua. “The Transnational Threat of Radicalization Through the Use of Online Gaming Platforms.” In *Fostering Innovation in the Intelligence Community*, edited by C. Gruber. Springer, in press.
- Blazakis, J., M. El Shawesh, N. Fink, L. McClintock, M. Saltskog, and Z. Schwitzky. *Quantifying the Q conspiracy: A Data-Driven Approach to Understanding the Threat Posed by QAnon*. The Soufan Center, 2021. <https://thesoufancenter.org/research/quantifying-the-q-conspiracy-a-data-driven-approach-to-understanding-the-threat-posed-by-qanon/>
- Borum, R. *Psychology of Terrorism*. Tampa, FL: University of South Florida, 2004.
- Borum, R. “Radicalization in Violent Extremism I: A Review of Social Science Theories.” *Journal of Strategic Security* 4, no. 4 (2011): 7–36. doi:10.5038/1944-0472441.
- Bowen, Andrew S. *Russian Military Intelligence: Background and Issues for Congress*. Congressional Research Service, November 15, 2021. <https://crsreports.congress.gov/product/pdf/R/R46616/7>.
- Bradbury, R., T. Bossomaier, and D. Kernot. “Predicting the Emergence of Self-Radicalization through Social Media: A Complex Systems Approach.” In *Terrorists' Use of the Internet*, edited by M. Conway, L. Jarvis, O. Lehané, S. Macdonald, and L. Nouri. IOS Press, 2017: 379–389. doi:10.3233/978-1-61499-765-8-379.
- Brewster, Jack. “Congress Will Get Its Second QAnon Supporter, as Boebert Wins Colorado House Seat.” *Forbes*, November 4, 2020. <https://www.forbes.com/sites/jackbrewster/2020/11/04/congress-will-get-its-second-qanon-supporter-as-boebert-wins-colorado-house-seat/?sh=348a5ef6568f>.
- Britzky, Hayley. “The US Military Is Still Struggling to Figure Out Social Media.” *Task & Purpose*, November 2, 2022. <https://taskandpurpose.com/news/military-social-media-challenges/>.
- Brown, O. “Right-Wing Extremism Online: Can We Use Digital Data to Measure Risk?” 2022. <https://crestresearch.ac.uk/comment/right-wing-extremism-online-can-we-use-digital-data-to-measure-risk/>
- Burgess, Matt. “A Deepfake Porn Bot Is Being Used to Abuse Thousands of Women.” *Wired*, October 2020, xx–xx.
- Campbell, Josh, and Jason Kravarik. “A 17-Year-Old Boy Died by Suicide Hours after Being Scammed. the FBI Says It’s Part of a Troubling Increase in ‘sextortion’ Cases.” *CNN*, 23 May 2022, www.cnn.com/2022/05/20/us/ryan-last-suicide-sextortion-california/index.html.

- Cook, Sarah, Angeli Datt, Ellie Young, and BC Han. *Beijing's Global Media Influence*. Freedom House, September 2022. <https://freedomhouse.org/report/beijing-global-media-influence/2022/authoritarian-expansion-power-democratic-resilience>.
- Council on Foreign Relations. *Demographics of the U.S. Military*. 2020. <https://www.cfr.org/backgrounder/demographics-us-military#:~:text=Now%2C%20there%20are%20about%201.3,percent%20of%20the%20U.S.%20population.&text=The%20army%20is%20the%20largest,marine%20corps%2C%20a nd%20coast%20guard>.
- Counter, J. "How the US Can Focus Its Fight Against Foreign Influence Operations." *Atlantic Council*, September 30, 2022. <https://www.atlanticcouncil.org/content-series/hybrid-warfare-project/how-the-us-can-focus-its-fight-against-foreign-influence-operations/>.
- The Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020, Pub. L. 116-92, 50 U.S.C. §3059.
- Dawson, J. (2023). Who controls the code, controls the system: Algorithmically Amplified Bullshit, Social Inequality, and the Ubiquitous Surveillance of Everyday Life. *Sociological Forum*, n/a(n/a). <https://doi.org/10.1111/socf.12907>.
- Defense Intelligence Agency. *North Korea Military Power: A Growing Regional and Global Threat*, October 15, 2021. <https://www.dia.mil/Portals/110/Documents/News/NKMP.pdf>.
- Department of Defense. "2020 Status of Forces Survey." *Annual Report on the Financial Literacy and Preparedness of Members of the Armed Forces*. Washington DC: Department of Defense, 3.
- Department of Defense. *Report on Predatory Lending Practices Directed at Members of the Armed Forces and their Dependents*, April 9, 2006.
- Department of Justice. *Justice News: Former U.S. Army Soldier Sentenced to 45 Years in Prison for Attempting to Murder Fellow Servicemembers in Deadly Ambush*. March 3, 2023. <https://www.justice.gov/opa/pr/former-us-army-soldier-sentenced-45-years-prison-attempting-murder-fellow-service-members>
- Dietary Supplement Health and Education Act of 1994, 103rd Cong. Pub. L. 103-417, 1994.
- Dixon, Stacy Jo. "Average Number of Hours per Day Spent on Select Social Media Platforms by Active-Duty Military Members in the United States as of February 2020." *Statista*, 2022. <https://www.statista.com/statistics/1130021/hours-spent-social-media-us-active-duty-military-members/>.
- Douglas, K. M., J. E. Uscinski, R. M. Sutton, A. Cichocka, T. Nefes, C. S. Ang, and F. Deravi. "Understanding Conspiracy Theories." *Political Psychology* 40, Suppl. 1 (2019): 1–33. doi:10.1111/pops.12568.
- Douglas, K. M.-W., and R. M Sutton. "Is the Label 'Conspiracy Theory' a Cause or a Consequence of Disbelief in Alternative Narratives?" *British Journal of Psychology* 113, no. 3 (2021): 1–16. doi:10.1111/bjop.12548.
- Eady, Gregory et al. "Exposure to the Russian Internet Research Agency Foreign Influence Campaign on Twitter in the 2016 US Election and Its Relationship to Attitudes and Voting

- Behavior.” *Nature Communications* 14, Article 62, January 9, 2023. <https://doi.org/10.1038/s41467-022-35576-9>.
- Eordogh, Fruzsina. “With Pizzagate, Is Cybersteria The New Normal?” *Forbes*, December 7, 2016. <https://www.forbes.com/sites/fruzsinaeordogh/2016/12/07/with-pizzagate-is-cybersteria-the-new-normal/?sh=3930d5e62b68>.
- Erickson, Sydney. “Deepfake Technology Poses a Threat to Reality.” *Journal of Gender, Race & Justice*, 3 Apr. 2023, jgrj.law.uiowa.edu/news/2023/04/deepfake-technology-poses-threat-reality.
- Eslick, A. N., L. K. Fazio, and E. J. Marsh. “Ironie Effects of Drawing Attention to Story Errors.” *Memory* 19 (2011): 184–191. doi:10.1080/09658211.2010.543908.
- Evans, Alexandra T., and Heather J. Williams. *How Extremism Operates Online*. Santa Monica, CA: RAND Corporation, 2022.
- Farokhmanesh, Megan. “The Debate on Deepfake Porn Misses the Point.” *Wired*, 1 Mar. 2023, www.wired.com/story/deepfakes-twitch-streamers-qtcinderella-atric-pokimane/.
- Fazio, L. “Pausing to Consider Why a Headline Is True or False Can Help Reduce the Sharing of False News.” *The Harvard Kennedy School Misinformation Review* 1, no. 2 (2020): 1–8. doi:10.37016/mr-2020-009.
- Federal Bureau of Investigation and Department of Homeland Security (DHS). *Strategic Intelligence Assessment and Data on Domestic Terrorism*. 2021.
- Federal Trade Commission. “FTC Takes Action against the Operators of Copycat Military Websites.” September 6, 2018. <https://www.ftc.gov/news-events/news/press-releases/2018/09/ftc-takes-action-against-operators-copycat-military-websites>.
- Federal Trade Commission. “Prepared Statement of the Federal Trade Commission: Protecting Military Servicemembers and Veterans from Financial Scams and Fraud, Before the Committee on Oversight and Reform Subcommittee on National Security.” July 13, 2022.
- Financial Literacy Training: Financial Services, 10 U.S.C. §992, (2023).
- Furnell, S. M., and M. J. Warren. “Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?” *Computers & Security* 18 no. 1 (1999): 28–34. doi: 10.1016/S0167-4048(99)80006-6.
- Gallacher, John D., Vlad Barash, Philip N. Howard, and John Kelly. “Junk News on Military Affairs and National Security: Social Media Disinformation Campaigns Against US Military Personnel and Veterans.” *Data Memo 2017.9*. Oxford, UK: Project on Computational Propaganda, 2017. <http://comprop.oii.ox.ac.uk/research/working-papers/vetops/>.
- Garamone, J. “New Strategy Seeks to Reinvigorate Deterrence in a Changing World.” *DOD News*, November 7, 2022. <https://www.defense.gov/News/News-Stories/Article/Article/3212005/new-strategy-seeks-to-reinvigorate-deterrence-in-a-changing-world/#:~:text=China%20is%20the%20pacing%20threat,is%20fundamentally%20changing%2C%20Kahl%20said>.

- Gaudette, Tiana, Ryan Scrivens, and Vivek Venkatesh. "The Role of the Internet in Facilitating Violent Extremism: Insights from Former Right-Wing Extremists." *Terrorism and Political Violence* 34, no. 7 (2022): 1339–1356. doi: 10.1080/09546553.2020.1784147.
- Gershaneck, Kerry. *To Win without Fighting: Defining China's Political Warfare*. Quantico, VA: Marine Corps University Press, 2020. <https://doi.org/10.36304/ExpwMCUP.2020.04>.
- Giusti, Serena, and Piras, Elisa. "Democracy and Fake News: Information Manipulation and Post-Truth Politics." ResearchGate. https://www.researchgate.net/publication/342946132_democracy_and_fake_news_information_manipulation_and_post-truth_politics.
- Global Engagement Center. *Disinformation Roulette: The Kremlin's Year of Lies to Justify an Unjustifiable War*. U.S. Department of State, February 23, 2023. <https://www.state.gov/disarming-disinformation/disinformation-roulette-the-kremlins-year-of-lies-to-justify-an-unjustifiable-war/>.
- Goldsmith, Kristofer. *An Investigation into Foreign Entities Who Are Targeting Servicemembers and Veterans Online*, Vietnam Veterans of American, 2019. <https://vva.org/wp-content/uploads/2019/09/VVA-Investigation.pdf>.
- Graddy, LaToya. "U.S. Army CID: Beware of 'hijacked' Webcam Scams." *Defense Visual Information Distribution Service*, 18 Oct. 2018, www.dvidshub.net/news/296868/us-army-cid-beware-hijacked-webcam-scams.
- Haard, Jenifer, Michael D. Slater, and Marilee Long. "Scientese and Ambiguous Citations in the Selling of Unproven Medical Treatments." *Health Communication* 16, no. 4 (2004): 411.
- Hafez, M. "Radicalization in the Persian Gulf: Assessing the Potential of Islamist Militancy in Saudi Arabia and Yemen." *Dynamics of Asymmetric Conflict* 1 (2008): 6–24.
- Haiminis, Itay. "Iran's Information Warfare." In *The Cognitive Campaign: Strategic and Intelligence Perspectives*, edited by Yossi Kuperwasser and David Siman-Tov, 135–147. Institute for National Security Studies and The Institute for the Research of the Methodology of Intelligence, 2019. https://www.terrorism-info.org.il/app/uploads/2019/11/H_259_19.pdf.
- Hale, W. Chris. "Extremism on the World Wide Web." *Criminal Justice Studies* 25, no. 4 (2012): 343–356.
- Helmus, Todd C., Ryan Andrew Brown, and Rajeev Ramchand. "Bum-Rushing Extremists From the Military Might Not Help." *Defense One*, 2021. <https://www.defenseone.com/ideas/2021/03/bum-rushing-extremists-military-might-not-help/172740/>.
- Human Rights First. *"Digital Soldiers": QAnon Extremists Exploit U.S. Military, Threaten Democracy*. Washington, DC: Human Rights First, 2022. https://humanrightsfirst.org/wp-content/uploads/2022/12/Digital-Soldiers_QAnon-Report.pdf
- Institute for Strategic Dialogue and the Global Disinformation Index. *Bankrolling Bigotry: An Overview of the Online Funding Strategies of American Hate Groups*. London: Institute for Strategic Dialogue, 2020. <https://www.isdglobal.org/isd-publications/bankrolling-bigotry/>.

- Jackson, Sam. *Oath Keepers: Patriotism and the Edge of Violence in a Right-Wing Antigovernment Group*. New York: Columbia University Press, 2020.
- Jakubowski, G. “What’s Not to Like? Social Media as Information Operations Force Multiplier.” *Joint Forces Quarterly*, July 1, 2019. <https://ndupress.ndu.edu>.
- Jensen, Michael, Elizabeth Yates, and Sheehan Kane. *Research Brief: Extremism in the Ranks and After*. College Park, MD: National Consortium for the Study of Terrorism and Response to Terrorism, 2021.
- Jensen, Michael, and Sheehan Kane. “QAnon-Inspired Violence in the United States: An Empirical Assessment of a Misunderstood Threat.” *Behavioral Sciences of Terrorism and Political Aggression*, 2021. doi: 10.1080/19434472.2021.2013292.
- Jensen, Michael, and Sheehan Kane. *Research Brief: QAnon Offenders in the United States*. College Park, MD: National Consortium for the Study of Terrorism and Response to Terrorism, 2021.
- Jensen, Michael, Sheehan Kane, and Elena Akers. *Research Brief: Profiles of Individual Radicalization in the United States (PRIUS): Mass Casualty Extremist Offenders with U.S. Military Backgrounds*. College Park, MD: National Consortium for the Study of Terrorism and Response to Terrorism, 2023.
- Jerit, J., and Y. Zhao. “Political Misinformation.” *Annual Review of Political Science* 23 (2020): 77–94. doi:10.1146/annurev-polisci-050718-032814.
- Joint Chiefs of Staff. “Joint Publication (JP) 3-04, Information in Joint Operations.” 2022. III-25. https://jdeis.js.mil/jdeis/new_pubs/jp3_04.pdf.
- Jones, Seth, Catrina Doxsee, Grace Hwang, and Jared Thompson. “The Military, Police, and the Rise of Terrorism in the United States.” *CJIS Briefs* (April). Washington, DC: Center for Strategic and International Studies, 2021.
- Kang, Cecilia. “Fake News Onslaught Targets Pizzeria as Nest of Child-Trafficking.” *The New York Times*, November 21, 2016. <https://www.nytimes.com/2016/11/21/technology/fact-check-this-pizzeria-is-not-a-child-trafficking-site.html>
- Karimi, Faith. “He Lost His Son to Suicide after a ‘Sextortion’ Scam. Now This Lawmaker Is Fighting to Save Other Teens.” *CNN*, 13 May 2023, www.cnn.com/2023/05/13/us/brandon-guffey-gavin-sextortion-law-cec/index.html#:~:text=In%202022%2C%20law%20enforcement%20agencies,by%20suicide%2C%20the%20FBI%20says.
- Keatinge, Tom, Florence Keen, and Kayla Izenman. “Fundraising for Right-Wing Extremist Movements.” *The RUSI Journal* 164, no. 2 (2019): 10–23. doi: 10.1080/03071847.2019.1621479.
- Kelkar, Shreeharsh. Post-Truth and the Search for Objectivity: Political Polarization and the Remaking of Knowledge Production. Engaging Science, Technology, and Society. <https://estsjournal.org/index.php/ests/article/view/286>.
- Klein, Kristen, and Arie Kruglanski. “Commitment and Extremism: A Goal Systemic Analysis.” *Journal of Social Issues* 69, no. 3 (2013): 419–435.

- Koehler, Daniel. "The Radical Online: Individual Radicalization Processes and the Role of the Internet." *Journal for Deradicalization*, 1 (2014/2015): 116–134.
- Kurilla, Michael, Gen U.S. Army. "Statement on the Posture of USCENTCOM - SASC Hearing." March 16, 2023. <https://www.centcom.mil/ABOUT-US/POSTURE-STATEMENT/>.
- Lacassagne, D., J. Béna, and O. Corneille. "Is Earth a Perfect Square? Repetition Increases the Perceived Truth Of Highly Implausible Statements." *Cognition* 223 (2022): 105052.
- Lamothe, Dan. "U.S. Military Social Media Accounts Apparently Hacked by Islamic State Sympathizers." *The Washington Post*, January 12, 2015. <https://www.washingtonpost.com/news/checkpoint/wp/2015/01/12/centcom-twitter-account-apparently-hacked-by-islamic-state-sympathizers/>.
- Lesser, Ian O., Bruce Hoffman, John Arquilla, David Ronfeldt, Michele Zanini, and Brian Michael Jenkins. *Countering the New Terrorism*. Santa Monica, CA: RAND Corporation, 1999.
- Levinsson, A., C. Miconi, Z. Li, R. L. Frounfelker, and C. Rousseau, "Conspiracy Theories, Psychological Distress, and Sympathy for Violent Radicalization in Young Adults during the COVID-19 Pandemic: A Cross-Sectional Study." *International Journal of Environmental Research and Public Health* 18 (2021): 7846–7858. doi:10.3390/ijerph18157846.
- Lucas, Ryan. "How Russia Used Facebook To Organize 2 Sets of Protesters." National Public Radio, November 1, 2017. <https://www.npr.org/2017/11/01/561427876/how-russia-used-facebook-to-organize-two-sets-of-protesters>.
- McClain, Colleen. "From Looking for Love to Swiping the Field: Online Dating in the U.S." *Pew Research Center: Internet, Science & Tech*, 2 Feb. 2023, www.pewresearch.org/internet/2023/02/02/from-looking-for-love-to-swiping-the-field-online-dating-in-the-u-s/.
- Merchant, N., U.S. Delays Intelligence Center Targeting Foreign Influence, *Federal News Network*, January 10, 2022, accessed June 29, 2022, <https://federalnewsnetwork.com/workforce/2022/01/us-delays-intelligence-center-targeting-foreign-influence/>, overall classification is UNCLASSIFIED.
- Miller, Gregory D. "Blurred Lines: The New 'Domestic' Terrorism." *Perspectives on Terrorism*, 13, no. 3 (2019): 63–75.
- Mullaney, Samantha. "Everything Flows: Russian Information Warfare Forms and Tactics in Ukraine and the US Between 2014 and 2020." *The Cyber Defense Review* 7, no. 4 (Fall 2022). https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/12_Mullaney.pdf.
- National Counterterrorism Center. *Domestic Terrorism Conference Report*. Washington DC: National Counterterrorism Center, 2020.
- National Defense Authorization Act for Fiscal Year 2006. 109th Congress Pub. L. 109-163. 2006.
- National Defense Authorization Act for Fiscal Year 2013. 112th Cong. Pub. L. 112-239. January 2, 2013.

- National Defense Authorization Act for Fiscal Year 2016. 114th Cong. Pub. L. 114-92. November 25, 2015.
- National Public Radio. “The Jan. 6 Attack: The Cases behind the Biggest Criminal Investigation in U.S. History.” 2023. <https://www.npr.org/2021/02/09/965472049/the-capitol-siege-the-arrested-and-their-stories>.
- National Security Agency. “NSA Cybersecurity Advisories and Guidance.” <https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/>. Overall classification is UNCLASSIFIED.
- National Security Agency. “NSA Cybersecurity Advisories and Guidance, Telework and Mobile Security.” <https://www.nsa.gov/Press-Room/Telework-and-Mobile-Security-Guidance/smdsort14639/title/>. Overall classification is UNCLASSIFIED.
- National Terrorism Advisory System Bulletin. “Summary of Terrorism-Related Threat to the United States.” 2023. <https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-may-24-2023>.
- Naval Criminal Investigative Services. “Cybersecurity: Sextortion, Exploitation of U.S. Servicemembers.” *NCIS Sextortion Brochure*. www.ncis.navy.mil/Portals/25/Documents/Media/NCIS%20Sextortion%20Brochure_V2.pdf?ver=2019-10-24-091534-483.
- Neumann, Peter R. “The Trouble with Radicalization.” *Internal Affairs* 89, no. 4 (2013): 873–893.
- Nigeria, News Agency of. “EFCC Wants Nigerian Brothers Extradited to U.S. over Sextortion.” *Peoples Gazette*, 9 May 2023, gazettengr.com/efcc-wants-nigerian-brothers-extradited-to-u-s-over-sex-tortion/.
- Office of the Assistant Secretary of Defense for Public Affairs. DoDI 5400.17, “Official Use of Social Media for Public Affairs Purposes.” Washington DC: Department of Defense, August 12, 2022. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/540017p.PDF>.
- Office of the Chief Information Officer. DoDI 8170.01, “Online Information Management and Electronic Messaging.” Washington DC: Department of Defense, January 2, 2019. https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Personnel_Related/22-F-0350_DODI_8170.01-Online_Information_Management_and_Electronic_Messaging_2Jan2019_CH-1_24Aug2021.pdf.
- Office of the Deputy Assistant of Defense for Military Community and Family Policy. *2021 Demographics: Profile of the Military Community*. 2021.
- Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community*, February 6, 2023. <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2023/item/2363-2023-annual-threat-assessment-of-the-u-s-intelligence-community>.

- Office of the Director of National Intelligence. *Assessing Russian Activities and Intentions in Recent US Elections*, January 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.
- Office of the Director of National Intelligence. *Intelligence Community Directive 204: National Intelligence Priorities Framework*. 2021. <https://www.dni.gov>. Overall classification is UNCLASSIFIED.
- Office of the Secretary of Defense. *Military and Security Developments Involving the PRC*. Washington, DC: Department of Defense, November 29, 2022. <http://defense.gov/CMPR>
- Office of the Under Secretary of Defense for Personnel and Readiness. DoD Instruction 1344.09, “Indebtedness of Military Personnel.” February 1, 2022, <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/134409p.pdf>.
- Patchin, Justin W., and Sameer Hinduja. “Sextortion among Adolescents: Results from a National Survey of U.S Youth” *Sexual Abuse* 32, no. 1 (2018): 30–54. journals.sagepub.com/doi/full/10.1177/1079063218800469.
- Paul, Christopher, and Miriam Matthews. *The Russian “Firehose of Falsehood” Propaganda Model*. RAND Corporation, 2016. <https://www.rand.org/pubs/perspectives/PE198.html>.
- Perliger, A. “Deciphering the Second Wave of the American Militia Movement.” *CARR Policy Insight*. Center for Analysis of the Radical Right, January 2021.
- Prichard, A. J., S. Powell, and T. Horr. *2022 IAVA Member Survey*. Syracuse, NY: Iraq and Afghanistan Veterans of America (IAVA) & D’Aniello Institute for Veterans and Military Families (IVMF), Syracuse University, 2022. https://iava.org/wp-content/uploads/2022/03/2022_IAVA_Member_Survey.pdf.
- Public Religion Research Institute. *The Persistence of QAnon in the Post-Trump Era: An Analysis of Who Believes in the Conspiracies*. 2022. <https://www.prrri.org/research/the-persistence-of-qanon-in-the-post-trump-era-an-analysis-of-who-believes-the-conspiracies/>.
- Report on the Military Lending Act and the Effects of High Interest Rates on Readiness, Response to House Report 116-442, Title V, May 2021, 7, 121.
- Riehle, Kevin P. *Russian Intelligence: A Case-based Study of Russian Services and Missions Past and Present*. National Intelligence University, Spring 2022. https://ni-u.edu/wp/wp-content/uploads/2022/05/Riehle_Russian-Intelligence.pdf.
- Rothschild, M. *The Storm Is Upon Us: How QAnon Became a Movement, Cult, and Conspiracy Theory of Everything*. Melville House, 2021.
- Rousis, G. J., F. D. Richard, and D.-Y. D. Wang. “The Truth Is Out There: The Prevalence of Conspiracy Theory Use By Radical Violent Extremist Organizations.” *Terrorism and Political Violence* (2020): 1–19. doi:10.1080/09546553.2020.1835654.
- Rottweiler, B., and P. Gill. “Conspiracy Beliefs and Violent Extremist Intentions: The Contingent Effects of Self-Efficacy, Self-Control, and Law-Related Morality.” *Terrorism and Political Violence* 34, no. 7 (2020): 1–20. doi:10.1080/09546553.2020.18003288

- Ryan, MacKenzie. “‘A White Nationalists Pyramid Scheme’: How Patriot Front Recruits Young Members.” *The Guardian*, September 2, 2022. <https://www.theguardian.com/us-news/2022/sep/02/patriot-front-recruits-members-young-pyramid-scheme>.
- Sacco, Lisa N. *Sifting Domestic Terrorism from Hate Crime and Homegrown Violent Extremism*. Congressional Research Service: Washington, DC, 2021.
- Safer-Lichtenstein, Aaron, Gary LaFree, Michael Jensen, and Patrick James. *Research Brief: The Use of Social Media by United States Extremists*. College Park, MD: START, 2018.
- Sarit Barzilai & Clark A. Chinn (2020) A review of educational responses to the “post-truth” condition: Four lenses on “post-truth” problems, *Educational Psychologist*, 55:3, 107-119, DOI: 10.1080/00461520.2020.1786388
- Scruton, Roger. *The Palgrave Macmillan Dictionary of Political Thought*, 3rd edition. 2007.
- Sherman, Justin and others. “Executive Summary: Duke University Research Project on Data Brokers, Data on U.S. Military, and Risks to U.S. National Security.” Duke University Sanford School of Public Policy, April 11, 2023.
- Silinsky, Mark. *Iran’s IRGC: Its Foreign Policy and Foreign Legion*. Quantico, VA: Marine Corps University Press, September 16, 2019. <https://doi.org/10.36304/ExpwMCUP.2019.01>.
- Simi, Pete, Steven Windisch, and Karyn Sporer. *Recruitment and Radicalization among U.S. Far Right Terrorists*. College Park, MD: START, 2016. https://www.start.umd.edu/pubs/START_RecruitmentRadicalizationAmongUSFarRightTerrorists_Nov2016.pdf
- Smith, Laura. “Lone Wolves Connected Online: A History of Modern White Supremacy.” *New York Times*, 2021.
- Smith, Tim. “Federal Probe of ‘sextortion’ Scheme Targeting Servicemen Leads to SC Prisoner Indictments.” *The Greenville News*, 28 Nov. 2018, www.greenvilleonline.com/story/news/local/south-carolina/2018/11/28/probe-sextortion-scheme-targeting-servicemen-leads-indictments/2135657002/.
- “Soldiers As Consumers: Predatory and Unfair Business Practices Harming the Military Community, Hearing before the Committee on Commerce, Science, and Transportation,” S. Hrg. 113-362, November 20, 2013, <https://www.govinfo.gov/content/pkg/CHRG-113shrg89464/html/CHRG-113shrg89464.htm>.
- Sotlar, Andrej. “Some Problems with a Definition and Perception of Extremism within a Society.” In *Handbook of Policing in Central and Eastern Europe*, edited by Gorazd Meško Charles B. Fields, Branko Lobnikar, and Andrej Sotlar, 1-5. New York: Springer, 2004.
- Speckhard, Anne, Molly Ellenberg, and T. M. Garrett. *The Challenge of Extremism in the Military is not Going Away without a New Perspective*. International Center for the Study of Violent Extremism, 2021.
- Squire, Megan, Jeff Tischauser, and Michael Edison Hayden. “One in Five Patriot Front Applicants Claim Military Ties.” Southern Poverty Law Center Hate Watch, 2022. <https://www.splcenter.org/hatewatch/2022/02/01/one-five-patriot-front-applicants-claim-military-ties>.

- Tenbarge, Kat. “Found through Google, Bought with Visa and MasterCard: Inside the Deepfake Porn Economy.” *NBCNews.Com*, 27 Mar. 2023, www.nbcnews.com/tech/internet/deepfake-porn-ai-mr-deep-fake-economy-google-visa-mastercard-download-rcna75071.
- “The Foreign Malign Influence Center” Office of the Director of National Intelligence, accessed June 29, 2023, <https://www.dni.gov/index.php/fmic-home>, overall classification is UNCLASSIFIED.
- “Three Nigerian Men Awaiting Extradition for Committing Sexual Extortion.” *Western District of Michigan | Three Nigerian Men Awaiting Extradition For Committing Sexual Extortion | United States Department of Justice*, 3 May 2023, www.justice.gov/usao-wdmi/pr/2023_0503_Sextortion_Indictment.
- Theohary, Catherine. “Information Warfare: Issues for Congress.” Congressional Research Service, March 5, 2018. <https://crsreports.congress.gov/product/pdf/R/R45142/5>.
- Topor, Lev, and Alexander Tabachnik. “Russian Cyber Information Warfare: International Distribution and Domestic Control.” *Journal of Advanced Military Studies* 12, no.1 (Spring 2021). <https://doi.org/10.21140/mcu.j.20211201005>.
- Trip, Simona, et al. “Psychological Mechanisms Involved in Radicalization and Extremism: A Rational Emotive Behavioral Conceptualization.” *Frontiers in Psychology*, 10, no. 437 (2010): 1–8.
- Ueda, Peter, et al. “Trends in Frequency of Sex and Number of Sexual Partners among US Adults Aged 18 to 44 Years.” *JAMA Network Open*, 12 June 2020, jamanetwork.com/journals/jamanetworkopen/article-abstract/2767066.
- “Understanding Fake Sextortion Email Scams.” *Netsafe*, December 2, 2021, netsafe.org.nz/faketortian-email-scam/.
- U.S. Department of the Air Force. *Foundational Competencies: Digital Literacy*, 2021. <https://www.af.mil/News/Article-Display/Article/2773797/foundational-competencies-digital-literacy/>.
- U.S Department of Defense. *Report: Enhancement of Protections on Consumer Credit for Members of the Armed Forces and Their Dependents*. https://consumerfed.org/pdfs/140429_dod_report.pdf, April 2014.
- U.S. Department of Education. “90/10 – Questions and Answers.” 2009. <https://www2.ed.gov/policy/highered/reg/hearulemaking/2009/90-10-q-and-a.html>.
- U.S. Senate Select Committee on Intelligence. *Russian Active Measures Campaigns and Interference in the 2016 U.S. Elections*. 116th Congress 1st Session, Report 116-XX, August 2020. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.
- Veterans Legal Clinic. *Underserved: How the VA Wrongfully Excludes Veterans with Bad Paper*. San Francisco, CA: Veterans Legal Clinic, 2016.
- Ware, Jacob, and Ania Zolyniak. “Jan. 6 and Beyond: Why the U.S. Should Pass Domestic Terrorism Legislation.” *Lawfare* (May 28, 2023). <https://www.lawfareblog.com/jan-6-and-beyond-why-us-should-pass-domestic-terrorism-legislation>.

- The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. 116th Cong. Pub. L. 116-283. January 1, 2021.
- Walker, Shaun. “Russian Troll Factory Paid US Activists to Help Fund Protests During Election.” *The Guardian*, October 17, 2017.
<https://www.theguardian.com/world/2017/oct/17/russian-troll-factory-activists-protests-us-election>.
- Weinberg, D., and Dawson, J. (2021). Military Narratives and Profiles in Russian Influence Operations on Twitter. 18th International Conference on Cyber Warfare and Security (ICCWS 2023), Maryland. SocArXiv. <https://doi.org/10.31235/osf.io/b9a2m>.
- Williams, Heather J and McCulloch, Caitlin. “Truth Decay and National Security.” The RAND Blog. <https://www.RAND.org/blog/2023/08/truth-decay-and-national-security.html>
- Wolfowicz, Michael, Yael Litmanovitz, David Weisburd, and Badi Hasasi, “Cognitive and Behavioral Radicalization: A Systematic Review of the Putative Risk and Protective Factors.” *Campbell Systematic Reviews* 16 (2020): e1102.
- Yamaguchi, Shinji, Masaaki Yatsuzuka, and Rira Momma. “China’s Quest for Control of the Cognitive Domain and Gray Zone Situations.” *China Security Report 2023*. Tokyo, Japan: National Institute for Defense Studies Japan, 2022.
<http://www.nids.mod.go.jp/english/publication/chinareport/index.html>.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YY) 00-11-23		2. REPORT TYPE Final		3. DATES COVERED (From – To)	
4. TITLE AND SUBTITLE Study on Cyberexploitation and Online Deception of Members of the Armed Forces and Their Families – Public Version				5a. CONTRACT NUMBER HQ0034-19-D-0001	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBERS	
6. AUTHOR(S) Jordan A. Adams-Leavitt, Michelle G. Albert, Sujeta B. Bhatt, Scott Cunningham, Shane Gillies, Janna R. Mantua, Ian W. McDaniel, Alexander Rios, Allison J. Savoy-Logan, Grace H. Spinner				5d. PROJECT NUMBER BC-5-5196	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES Institute for Defense Analyses 730 East Glebe Road Alexandria, VA 22305				8. PERFORMING ORGANIZATION REPORT NUMBER IDA Product 3001914	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Christine Condon, DoD Deputy Chief Information Officer for Resources and Analysis Department of Defense Chief Information Officer 6000 Defense Pentagon Washington, D.C. 20301-6000				10. SPONSOR'S / MONITOR'S ACRONYM DoD CIO	
				11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution Statement A. Approved for public release: distribution is unlimited.					
13. SUPPLEMENTARY NOTES Project Leader: Thomas M. Kelso					
14. ABSTRACT The U.S. Military is vulnerable to information operations from our adversaries. The emergence of new technologies, such as artificial intelligence (AI) and AI-enabled “deepfakes,” coupled with social media algorithms and the commercial data marketplace, enable very precise targeting of personnel and can aggregate such targeting at a scale that can disrupt readiness of our military forces. The consequence of precision targeting at scale can have significant impact on the Department of Defense (DoD). The 2021 National Defense Authorization Act (NDAA) directed the Secretary of Defense to conduct a study into this topical area and provide a report back to the Congressional Committees. The Deputy DoD Chief Information Officer (CIO) for Resources and Analysis tasked IDA with conducting the resultant study and providing the results. The NDAA language directed many aspects of the study.					
15. SUBJECT TERMS Cyberexploitation, Online Deception, Deepfake, Social Media Algorithms, Commercial Data, Information Operations					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Unlimited	18. NUMBER OF PAGES 112	19a. NAME OF RESPONSIBLE PERSON Christine Condon, DoD Deputy Chief Information Officer for Resources and Analysis
					19b. TELEPHONE NUMBER (Include Area Code) 703-697-7627
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			

