The US Army War College Quarterly: Parameters

Volume 52
Number 1 *Volume 52, Number 1 (2022)*

Article 9

Spring 3-9-2022

Information Warfare: Lessons in Inoculation to Disinformation

Meghan Fitzpatrick

Ritu Gill

Jennifer F. Giles

Information Warfare: Lessons in Inoculation to Disinformation

Meghan Fitzpatrick, Ritu Gill, and Jennifer F. Giles

ABSTRACT: While propaganda and disinformation have been used to destabilize opposing forces throughout history, the US military remains unprepared for the way these methods have been adapted to the Internet era. This article explores the modern history of disinformation campaigns and the current state of US military readiness in the face of campaigns from near-peer competitors and proposes education as the best way to prepare US servicemembers to defend against such campaigns.

Keywords: propaganda, disinformation, media literacy, military education, inoculation

Propaganda and disinformation are powerful tools of influence. The former can be defined as "deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist."[1] Meanwhile, the latter is a "deception technique based on the dissemination of untrue information with the intention to deceive, manipulate and mislead," exploiting human emotions as a means of influence.[2] Throughout the twentieth century, allies and adversaries have employed these tools to achieve their strategic goals. American President Dwight D. Eisenhower repeatedly recognized the chance of an "all out shooting war is far less than the danger we face on a political warfare front."[3] And, today's digital landscape means false narratives can spread further and faster than ever before.

Indeed, there is evidence countries like Russia have already made a significant impact on rival nations through these tactics. Numerous scholars point to the 2016 US presidential election as a prime example.[4] In these instances, disinformation relies on exploiting preexisting tensions in a target society (for example, race,

1. Garth S. Jowett and Victoria O'Donnell, *Propaganda & Persuasion*, 6th ed. (Newbury Park, CA: Sage Publications, 2015), 7.

2. Matthew Duncan et al., *Coronavirus and Disinformation: Narratives, Counter-strategies and the Inoclation of Audiences*, DRDC-RDDC-2020-L096 (Ottawa, ON: Defense Research and Development Canada, April 2020), 1.

3. President Dwight D. Eisenbower as quoted in Kenneth A. Osgood, "Form before Substance: Eisenhower's Commitment to Psychological Warfare and Negotiations with the Enemy," *Diplomatic History* 24, no. 3 (Summer 2000): 405.

4. *Disinformation: A Primer in Russian Active Measures and Influence Campaigns: Hearings before the Select Committee on Intelligence of the United States Senate Panel II*, 115th Cong. (2017) (statement of Thomas Rid, Professor of Security Studies), https://www.govinfo.gov/content/pkg/CHRG-115shrg25998/html/CHRG-115shrg25998.htm.

ethnicity, and class) to create division. As a result, these narratives frequently place vulnerable communities at risk and put institutions made up of diverse groups under strain, including the US military, which draws on Americans from all social, cultural, religious, political, and economic backgrounds.

Disinformation poses a threat to these kinds of organizations and by extension, countries. In 2019, the United Kingdom's cross-party committee on Digital Culture, Media, and Sport described the spread of false information online as an existential threat to democracy.[5] The gravity of this challenge requires close analysis. This article argues education is the optimal strategy to counter disinformation, identifies lessons learned from nations that have been a target of disinformation, reviews the evolution of disinformation as a tactic of information warfare, looks at the psychological mechanisms through which adversaries manipulate online, assesses the threat disinformation poses to institutions like the military, and reflects on the potential education has to inoculate targeted groups and help everyone survive and thrive in an increasingly digital world.[6]

How Propaganda and Disinformation Work

State and nonstate actors have long used propaganda and disinformation to gain strategic advantage. The arrival of modern mass media in the early twentieth century, however, allowed their efforts to take on global dimensions.[7] During both world wars, propaganda was an important tool employed to achieve a range of goals. For example, radio allowed key leaders like American President Franklin D. Roosevelt and British Prime Minister Winston Churchill to address domestic audiences directly in their own homes, informing them and influencing their perceptions of the war. Film was similarly employed to boost morale and drive recruitment efforts. Directed by Oscar-winning filmmaker Frank Capra, the *Why We Fight* documentary series is still considered one of the best examples of such material. The impact of these efforts cannot be underestimated. Some historians even contend the information war unleashed by the Allies was central to victory. Messaging at home was combined alongside actions in the field by organizations like Britain's

5. House of Commons Digital, Culture, Media and Sport Committee, *Disinformation and 'Fake News': Final Report* (United Kingdom: House of Commons, 2019).

6. Ritu Gill et al., "Managing Cyber Risk to Mission: Disinformation in the Cyber Domain Detection, Impact and Counter Strategies," in *24th International Command and Control Research & Technology Symposium (ICCRTS) Proceedings* (Laurel, MD: International Command and Control Institute, 2019), 10; and Elinor Carmi et al., "Data Citizenship: Rethinking Data Literacy in the Age of Disinformation, Misinformation, and Malinformation," *Internet Policy Review* 9, no. 2 (2020): 2, 4–5.

7. Jowett and O'Donnell, *Propaganda & Persuasion*, 7.

Political Warfare Executive, which engaged in operations to undermine enemy propaganda, which proved increasingly out of sync with the reality of events.[8]

Throughout the Cold War, influence continued to play a central role, and disinformation formed a pivotal element of Soviet active measures, or "overt and covert techniques for influencing events and behaviour in, and the actions of, foreign societies," with estimates Warsaw Pact countries ran over 10,000 disinformation operations from 1945 to 1989.[9] No matter the form it takes, disinformation is intended to exploit an adversary's weaknesses.[10] As Thomas Rid of Johns Hopkins University explains, "the tried and tested way . . . is to use an adversary's existing weaknesses against himself, to drive wedges into *preexisting* cracks. The more polarized a society, the more vulnerable it is."[11]

Russia's use of disinformation campaigns continues to be a key part of its strategy and has taken on a new form in today's online ecosystem. Russian disinformation can be broken down into four "Ds"—dismiss, distort, dismay, and distract—to disrupt critical thinking.[12] Societies have trigger topics, ranging from immigration and abortion to race and religion, which are likely to incite an emotional response and even lead to what is called an amygdala hijack. This is a psychological term referring to when the part of a person's brain controlling emotion becomes so inflamed the person can no longer critically reason. In other words, people lose connection to the part of the brain governing reasoning and evaluation of facts.[13]

But emotionally charged narratives are only one way adversarial actors can exploit online audiences who often experience information overload.[14] The human brain, lacking capacity and time, cannot sift through all the information available.[15] This lack of time and cognitive resources means individuals cannot sort fact from fiction, and they use cognitive shortcuts to process information, making them susceptible to disinformation campaigns. For example, confirmation

8. Haroro J. Ingram, *A Brief History of Propaganda during Conflict: Lessons for Counter-Terrorism Strategic Communications* (Netherlands: International Centre for Counter-Terrorism, 2016), 18–19; and Meghan Fitzpatrick, "Sowing Discord, Countering Fear: Force Protection and Resilience to Disinformation," *Proceedings of the International Command and Control Research Technology Symposium* (November 2020), 2.

9. Roy Godson and Richard Shultz, "Soviet Active Measures: Distinctions and Definitions," *Defense Analysis* 1, no. 2 (1985), 102.

10. Meghan Fitzpatrick, *Pandemics and Prophylaxis: Lessons Learned from Pandemics Past about Countering Mis- and Disinformation (1918–2020)* (Ottawa: DRDC, 2020), 3.

11. *Disinformation: A Primer*, 2.

12. Ben Nimmo, "Anatomy of an Info-War: How Russia's Propaganda Machine Works and How to Counter It," Stop Fake, May 29, 2015, https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/, accessed February 13, 2019.

13. Daniel Goleman, *Emotional Intelligence: Why It Can Matter More than the IQ* (New York: Bantam, 1996); and Rebecca Goolsby, "Developing a New Approach to Cyber Diplomacy: Addressing Malign Information Maneuvers in Cyberspace," in *Senior Leadership Roundtable on Military and Defence Aspects of Border Security in South East Europe*, ed. Itamara V. Lochard (Washington, DC: IOS Press, 2019), 105–16.

14. Gill et al., "*Managing Cyber Risk*," 7.

15. Duncan et al., *Coronavirus and Disinformation*, 1–14.

bias involves searching for, interpreting, and recalling information consistent with one's beliefs and attitudes. Individuals accept information that is congruent with their perspective as opposed to taking the time to process information that is contradictory. For instance, a 2019 study in the journal *Science Advances* found individuals who lean toward conservative politics tend to share social media posts from Republicans.[16]

Online actors are further able to exploit biases using rapidly emerging technologies, including deepfakes or AI-manipulated audio or video content either AI-rendered, edited or recut, misappropriated, or misattributed. Deepfakes may increase the ability of malign actors to exploit emotions and cognitive biases.[17] Images have been found to be more impactful than text alone.[18] Words are "abstract symbols that need to be reconstructed into a mental image of reality."[19] In contrast, images appear to offer a direct reference to reality that reduces the suspicion of manipulation.

Armed Forces and Disinformation

Like the nation it protects, the US military is increasingly diverse. Women made up 16 percent of the active-duty force in 2017, and ethnic minorities currently comprise 42 percent of military personnel.[20] This diversity can leave the military, like the country at large, vulnerable to disinformation campaigns. These campaigns represent a serious challenge to operational security and the overall cohesion of the armed forces, their allies, and the wider defense community.

For example, adversaries have consistently targeted the forces making up NATO's Enhanced Forward Presence in Estonia, Latvia, Lithuania, and Poland. In 2020, Russian-sponsored actors released a forged letter online where Polish Brigadier General Ryszard Parafianowicz appeared to criticize openly the American presence in his country during the US-led exercise Defender-Europe 20. During the same exercise, Russian sources also claimed the US military had ignored COVID-19–related travel restrictions, even though US officials had reduced the size and scope of Defender-Europe 20 due to public

16. Andrew Guess, Jonathan Nagler, and Joshua Tucker, "Less Than You Think: Prevalence and Predictors of Fake News Dissemination on Facebook," *Science Advances* 5, no. 1 (2019): 1–8.
17. Robert Chesney and Danielle K. Citron, "Disinformation on Steroids: The Threat of Deep Fakes," *Digital and Cyberspace Policy Program*, Council on Foreign Relations, October 16, 2018, https://www.cfr.org/report/deep-fake-disinformation-steroids.
18. Michael Hameleers et al., "A Picture Paints a Thousand Lies? The Effects and Mechanisms of Multimodal Disinformation and Rebuttals Disseminated via Social Media," *Political Communication* 37, no. 2 (2020): 281–301.
19. Hamleers, 297.
20. Amanda Barroso, "The Changing Profile of the U.S. Military: Smaller in Size, More Diverse, More Women in Leadership," Pew Research Center, September 10, 2019, https://www.pewresearch.org/fact-tank/2019/09/10/the-changing-profile-of-the-u-s-military/.

health considerations.[21] The threat of influence no longer exists only during deployment but also in garrison because of "the collapsed nature of communication . . . and . . . porous boundaries between war and everyday life," which means geography is no longer enough to act as a defense.[22]

Hostile actors consistently target members of the US armed forces and veteran communities online. Beginning in 2017, Vietnam Veterans of America, a congressionally chartered nonprofit organization, began a two-year investigative study and discovered, "persistent, pervasive, and coordinated online targeting of American servicemembers, veterans, and their families by foreign entities."[23] The report demonstrated servicemembers and their social networks are vulnerable to disinformation. Foreign entities see members of the military community, who often have access to confidential and classified materials, as an attractive target. What is more, active members and veterans are a significant influence demographic in US political life. A team of Vietnam Veterans of America researchers inspected hundreds of Facebook pages and social media accounts and found American servicemembers, veterans, and other social media followers of several veterans organizations were specifically targeted by foreign entities.[24] They also found individuals from over 30 countries administered the sites they reviewed, and that administrators of these imposter Facebook pages infiltrated other public and private groups.

Imposter pages and accounts built a following by impersonating legitimate military and veterans groups, like the Vietnam Veterans of America, and used camaraderie and community as a way to attract new members. This activity was so prolific Facebook shut down a third of the reviewed accounts for inauthentic behavior or "misleading actions to deceive others about who an individual/group is or what the individual or group is doing."[25] Before the shut down, the pages drew over 32 million users. Foreign administrators had used the platforms to "try to drive wedges between groups along varying racial or ethnic identities or prejudices, often pitting law enforcement against minorities."[26] This action frequently involved posting divisive content designed to polarize group members, from sharing pictures of NFL quarterback Colin Kaepernick to spreading false information about controversial public figures like

21. "NATO's Approach to Countering Disinformation: A Focus on COVID-19," NATO, updated July 17, 2020, https://nato.int/cps/en/natohq/177273.htm.
22. Lisa Ellen Silvestri, "Friended from the Front: Social Media and 21st Century War" (doctoral thesis, University of Iowa, May 2014), 6.
23. Kristofer Goldsmith, *An Investigation into Foreign Entities Who Are Targeting Servicemembers and Veterans Online* (Silver Spring, MD: Vietnam Veterans of America, 2021), 6.
24. Goldsmith, *Investigation into Foreign Entities*, 12; and Dominique Laferrière, Meghan Fitzpatrick, and Janani Vallikanthan, *An Ounce of Prevention, A Pound of Cure: Building Resilience to Disinformation* (Ottawa, ON: DRDC, 2022).
25. Goldsmith, *Investigation into Foreign Entities*, 18.
26. Goldsmith, *Investigation into Foreign Entities*, 35.

Congresswoman Alexandria Ocasio-Cortez and posting xenophobic statements like "VETS BEFORE ILLEGALS" to play on sensitive topics like immigration.[27] Disinformation targets fault lines within a society, and military personnel are not immune to these tactics.

Adversary disinformation campaigns undermine servicemembers' ability to discern fact from fiction. These campaigns penetrate their social networks and make them susceptible to conspiracy theories and extremist groups, which degrades unit cohesion and presents a real force protection threat. Although there are no indications an adversary was directly responsible for the US Capitol attack of 2021, years of influence operations culminated in a distorted cognitive environment—an alternate reality—for many who participated in the riots, and implanted a lasting social and political division that could continue for years.[28] Using the attack as an example, adversaries will continue active disinformation campaigns and employ all information domain tools to exacerbate discord and strengthen their position.[29] Russia has used digital media to fan the flames following the Capitol attack, and China's media has taken the opportunity to create false equivalencies to justify its behaviors and undermine faith in democratic processes and US legitimacy as a global leader.[30]

These effects offer clear evidence online conspiracy theories and disinformation do not remain online only but can and do culminate in violence. While disinformation is insidious and creates long-lasting effects at the national, strategic, and tactical levels, it can be mitigated through awareness and education.

Education: Inoculation to Disinformation?

There is debate about how to deal with disinformation. Mounting evidence from the humanities and social sciences suggests the best long-term solution is

27. Goldsmith, *Investigation into Foreign Entities*, 7, 38, 94, all caps in original.

28. Joan Donovan, "How Social Media's Obsession with Scale Supercharged Disinformation," *Harvard Business Review*, January 13, 2021, https://hbr.org/2021/01/how-social-medias-obsession-with-scale-supercharged-disinformation; and Scott Rosenberg, "Disinformation's Big Win," Axios, January 8, 2021, https://www.axios.com/disinformations-big-win-russia-trump-5e6a9cc6-4bfb-456d-9712-d97bd4b2a6cb.html.

29. Stratfor Analysts, "Opinion: For U.S. Adversaries Including Russia, Iran and China, the Capitol Siege Offers a Window of Opportunity," Stratfor (website), January 11, 2021, https://www.marketwatch.com/story/for-u-s-adversaries-including-russia-iran-and-china-the-capitol-siege-offers-a-window-of-opportunity-11610379131.

30. "After Capitol Riots, Russia Slams US's 'Archaic' Electoral System," *Al Jazeera* (website), January 7, 2021, https://www.aljazeera.com/news/2021/1/7/russian-officials-say-us-democracy-limping-after-capitol-riot; Agency France-Presse, "'Beautiful Sight': China Mocks US Capitol Siege Online, Recalls Nancy Pelosi's Remark on Hong Kong Protests," Firstpost (website), January 7, 2021, https://www.firstpost.com/world/beautiful-sight-china-mocks-us-capitol-siege-online-recalls-nancy-pelosis-remark-on-hong-kong-protests-9180311.html; and Tracy Wen Liu, "Chinese Media Calls Capitol Riot 'World Masterpiece'," *Foreign Policy* (website), January 8, 2021, https://foreignpolicy.com/2021/01/08/chinese-media-calls-capitol-riot-world-masterpiece/.

to educate the public to recognize disinformation.[31] Numerous organizations have stressed the value of education in combating hate. In 2018, the European Commission developed a digital literacy plan for implementation across the European Union.[32] The same year, the London School of Economics Truth, Trust, and Technology Commission called on the British government to incorporate media literacy as part of its national curriculum.[33] Although many countries have just begun to recognize and implement educational programs to counter disinformation campaigns, several countries have proven systems in place.

The Scandinavian and Baltic countries provide a template for how to implement these disinformation education programs. Their experience is unique since "Few [regions] have been subject to more consistent Russian information manipulation over the past four to five years," including Finland, which has been a consistent target of Kremlin-backed propaganda since becoming independent in 1917.[34] Analysts from RAND Europe argue several factors contribute to Finland's resilience to foreign influences, including high rates of media literacy.[35] The Finnish government has achieved media literacy through educational campaigns, including a 2014 initiative to teach students, journalists, politicians, and the public how to recognize fake news. Students in primary and secondary education were also tested on their ability to recognize deepfake videos and exercise critical-thinking skills. These programs, and others like them, are "just one layer of a cross-sector approach that Finland is taking to prepare citizens of all ages for the complex digital landscape."[36]

Working together toward a common goal, the Lithuanian government frequently partners with these groups to increase levels of academic research that survey the public on this issue, and media projects focused on debunking and fact-checking. It has also provided funding and/or support for the development

31. Ritu Gill, "Understanding Influence in the Digital Information Environment and the Impact on Audiences and Actors," (speaking notes, DRDC, Ottawa, ON, 2019).

32. Carmi et al., "Data Citizenship," 7–8.

33. Gianfranco Polizzi and Ros Taylor, *Misinformation, Digital Literacy and the School Curriculum*, Media Policy Brief 22 (London: London School of Economics and Political Science, 2019), 4-5.

34. Michael J. Mazarr et al., *Hostile Social Manipulation: Present Realities and Emerging Trends* (Santa Monica, CA: RAND Corporation, 2019), 210–11.

35. William Marcellino et al., *Human-Machine Detection of Online-Based Malign Information* (SantaMonica, CA: RAND Corporation, 2020), 11–13.

36. Marcellino et al., *Human-Machine Detection*, 13.

of an AI-driven platform to monitor media (Debunk.eu) and the creation of media literacy projects for vulnerable groups (elderly, minority populations).[37]

Disinformation surrounding the COVID-19 pandemic is a global issue and similarly to the Scandinavian and Baltic countries, other nations have taken effective countermeasures to address associated disinformation. The Taiwanese government collaborated with the Taiwan FactCheck Center.[38] As described by Gill and colleagues, Taiwan used a social-media platform similar to WhatsApp to disseminate accurate information to counter online disinformation.[39] Additionally, the government increased disinformation monitoring to prevent its spread and worked with Facebook to gray out disinformation on Facebook timelines. Lastly, guides were created on how to distinguish between real and fake accounts and suspicious and credible information. Lien and authors noted such collaboration, platforms, and guides were critical in fostering Taiwan's resilience to China's COVID-19 disinformation.[40]

Recommended US Military Media Literacy Training

The Department of Defense (DoD) must mandate a standardized, multifaceted media literacy program to provide servicemembers with the skills required to confront disinformation. The US population from which the armed forces recruit is significantly undertrained and underprepared to compete with disinformation. While a small minority of US schools teach media literacy, most youths and adults lack the skills to analyze critically the information they consume.[41] If this deficiency is not addressed, servicemembers will remain vulnerable to cognitive shortfalls, and ideological divisions will undermine force resiliency. While the Department of Defense has developed initiatives to train servicemembers to combat adversary influence, a combination of public-sector best practices and DoD resources can produce a more comprehensive program,

37. Vytautas Kersanskas, *Deterring Disinformation? Lessons from Lithuania's Countermeasures since 2014*, Hybrid Center of Excellence Paper 6 (Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2021), 10–12.

38. Ritu Gill et al., "Coronavirus: Gray Zone Tactics in Cyberspace" in *25th International Command and Control Research and Technology Symposium Proceedings* (Laurel, MD: International Command and Control Institute, 2020).

39. Ritu Gill et al., "Coronavirus: Gray Zone Tactics."

40. Yi-Ting Lien, "Why China's COVID-19 Disinformation Campaign Isn't Working in Taiwan," *Diplomat* (website), March 20, 2020, https://thediplomat.com/2020/03/why-chinas-covid-19-disinformation-campaign-isnt-working-in-taiwan/.

41. Media Literacy Now, "U.S. Media Literacy Policy Report 2020," January 6, 2020, https://medialiteracynow.org/u-s-media-literacy-policy-report-2020/.

consisting of an annual online training course and an in-person course, to arm DoD personnel and families against disinformation.

In 2018–19, the DoD Joint Staff developed and launched the Joint Knowledge Online (JKO) J3ST-US1396 Influence Awareness computer-based course. The 90-minute course educates participants on adversary and competitor initiatives to influence US and DoD personnel, discusses near-future challenges in the information environment, and briefly introduces tools to counter influence. The course is not mandatory or well advertised, and its static content is becoming stale as the information environment evolves. Although the course's primary objective is to increase awareness of online influence activities, it is prefabricated and inflexible, and its focus on crucial media literacy skills is underdeveloped. Participants cannot ask questions or practice the dynamic skills needed to develop healthy online information consumption habits on the personal devices used most often: cellphones, tablets, and laptops. In addition, the course does not assess participants or gather performance data to inform course refinement. These shortfalls critically hinder the course's ability to arm DoD personnel against disinformation. The incorporation of best practices from the public sector could mitigate these gaps.

The Department of Defense would greatly benefit from partnering with public-sector media literacy leaders to develop a dynamic in-person training program. Programs, such as the International Research Exchange Board's (IREX) Learn to Discern and the Stanford History Education Group's Civic Online Reasoning, are making great strides in meeting the challenges of the evolving information environment and offer many of the core media literacy skills servicemembers need. These private-sector programs provide the hands-on, real-world applications JKO lacks, such as practical exercises that test the ability to search for, evaluate, and verify information online and to make informed decisions using healthy media literacy habits while accessing personal devices. They also compel students to analyze consumption habits and take ownership of decisions to click, share, read, like, or interact with content online. Students leave the courses with a better understanding of how their actions shape the information environment of their friends, community, and the nation. These programs are designed to be taught by a facilitator through easily accessible, professionally guided in-person or online courses. The main shortcoming of these programs is they do not specifically address adversary and competitor disinformation efforts

that threaten servicemembers, though they could be tailored to meet these requirements in a partnership with the Department of Defense.[42]

Private-sector best practices and DoD resources could be combined to develop a comprehensive media literacy training program consisting of an annual online course and a small in-person class that would benefit DoD personnel and family members. The Joint Staff J-7 and its JKO training staff and platform are best positioned to develop and implement a computer-based media literacy training course across the force. Like annual cybersecurity training, all personnel—including civilians—should be required to complete the annual training that should establish a baseline of participants' media fluency and track changes across demographics. Participant performance data could inform course refinement and, similar to a command climate survey, the course could aggregate concerning trends for the attention of the service chiefs or higher, if necessary. The course should test the ability of servicemembers to demonstrate media literacy skills, such as differentiating between a fact and an opinion, verifying sources, identifying altered visual information, identifying imposter social media accounts, and recognizing targeted divisive material, and also instill a sense of responsibility when sharing or interacting with information online.

In addition to the computer-based training, the service components should also implement focused in-person media literacy training at the company level. Sessions should be held in small classrooms or town halls and led by DoD facilitators, from public affairs or communication strategy and operations, who have been trained by leading public-sector practitioners. The training should address trouble areas flagged by the annual computer-based class and facilitate practical application exercises that test the students' ability to recognize and counter disinformation using personal devices. The practical application exercises would model leading public-sector courses but would focus on DoD equities. The in-person class would also offer an opportunity for servicemembers to discuss ongoing adversarial cyberattacks, media influence, military actions, challenges faced by partners and allies, and foreign interference in domestic events.

In addition, family predeployment briefs should integrate media literacy training to increase awareness before a servicemembers' deployment. Although the Department of Defense cannot mandate family members take online media literacy training, many are concerned about the threat of false

42. "About Us," IREX, https://www.irex.org/about-us, accessed December 15, 2020; "Randomized Control Trial Finds IREX's Media Literacy Messages to Be Effective in Reducing Engagement with Disinformation," IREX, October 20, 2020, https://www.irex.org/news/randomized-control-trial-finds-irexs-media-literacy-messages-be-effective-reducing-engagement; and "Civic Online Reasoning Curriculum Collections," Stanford History Education Group, https://cor.stanford.edu/curriculum/.

information and welcome opportunities to understand and protect themselves from these threats.[43] Family readiness officers and key spouse leaders are also conduits to promote and share online media literacy education opportunities and encourage awareness.

Servicemembers and their families must learn and practice media literacy skills so they can protect themselves and counter adversary initiatives.[44] Awareness programs would help them realize the disinformation threat and encourage them to defend themselves.[45] A DoD-mandated, standardized, and multifaceted media literacy program that combines public-sector best practices and DoD equities can produce a comprehensive computer-based course and an in-person course that provides servicemembers and families the skills they need to confront adversary disinformation threats successfully.

Conclusion

The pace of technological acceleration and the division inherent in recent politics shows no signs of abating. As a result, the world will continue to face a proliferation of disinformation in online spaces, enhanced by sophisticated technology like deepfake videos.[46] These advancements make it difficult to determine attribution or debunk disinformation and create a serious threat to democratic institutions, which are increasingly diverse in composition.[47]

While decisionmakers have considered a variety of solutions, none are likely to have the lasting impact of thorough media literacy education.[48] In 2017, former "Chairman of the Joint Chiefs of Staff, General Joseph Dunford Jr. . . . designat[ed] information as the seventh joint warfare function."[49] For troops to be effective warriors, they must possess the skills needed to navigate a deceptive environment and recognize when and how they

43. Lloyd's Register Foundation/GALLUP, "The Lloyd's Register Foundation World Risk Poll," 2019 Executive Summary, 5, https://wrp.lrfoundation.org.uk/.

44. Peter W. Singer and Eric B. Johnson, "The Need to Inoculate Military Servicemembers against Information Threats: The Case for Digital Literacy Training for the Force," War on the Rocks, February 1, 2021, https://warontherocks.com/2021/02/we-need-to-inoculate-military-servicemembers-against-information-threats-the-case-for-digital-literacy-training/.

45. EU East StratCom Task Force, "25 Ways of Combatting Propaganda without Doing Counter-Propaganda," Euromaidan Press (website), June 16, 2017, https://euromaidanpress.com/2017/06/16/ways-of-combatting-propaganda-without-counter-propaganda/.

46. Robert Chesney and Danielle Citron, "Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics," *Foreign Affairs* 98, no. 1 (January/February 2019): 147, https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war.

47. Canadian Security Intelligence Service, *Who Said What? The Security Challenges of Modern Disinformation* (Ottawa: Government of Canada, 2018), 16–17.

48. Christopher Paul and Miriam Matthews, *Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It*, Perspective (Santa Monica, CA: RAND Corporation, 2016), 2.

49. Linton Wells II, "Cognitive-Emotional Conflict: Adversary Will and Social Resilience," *PRISM* 7, no. 2 (2017), 4–17, https://cco.ndu.edu/PRISM-7-2/Article/1401814/cognitive-emotional-conflict-adversary-will-and-social-resilience/.

are being manipulated online. In "Deepfakes and the New Disinformation War," Robert Chesney and Danielle Citron argue, "democracies will have to accept an uncomfortable truth: in order to survive the threat . . . they are going to have to learn how to live with lies."[50] If democratic societies are to function effectively, everyone will have to learn to survive and thrive in a complicated digital landscape.

Meghan Fitzpatrick

Dr. Meghan Fitzpatrick, a strategic analyst with Defence Research and Development Canada (DRDC) Centre for Operational Research and Analysis (CORA), is a widely published author on trauma and resilience. Her current work looks at how militaries are navigating the increasing importance of the information environment. Since joining DRDC, she has received recognition for her research, including the CORA Award for Outstanding Achievement in Defence Analysis.

Ritu Gill

Dr. Ritu Gill has a PhD in social psychology from Carleton University and is currently a section head with DRDC. Her research examines online influence activities, specifically, how the Internet and social media influences the information environment, including the analysis of online audiences, and how deception techniques employed by adversaries, such as disinformation, impact audiences. She has been part of international defence research collaborations and was co-lead for the NATO Human Factors and Medicine Research Task Group "Digital and Social Media Assessment for Effective Communication and Cyber Diplomacy."

Jennifer F. Giles

Major Jennifer F. Giles, US Marine Corps, is currently a communication strategy and operations officer, a foreign area officer who advises commanders' strategic and cultural engagement plans in the Pacific theater, and an instructor at the Marine Air-Ground Task Force Staff Training Program. She wrote *Disrupting Disinformation: Force Protection through Media Literacy Training* and recently spoke on media literacy and adversary disinformation for the Defense Information School "DINFOS Live."

50. Chesney and Citron, "Deepfakes and New Disinformation War," 155.

Select Bibliography

Godson, Roy, and Richard Shultz. "Soviet Active Measures: Distinctions and Definitions." *Defense Analysis* 1, no. 2 (1985).

Goldsmith, Kristofer. *An Investigation into Foreign Entities Who Are Targeting Servicemembers and Veterans Online*. Silver Spring, MD: Vietnam Veterans of America.

Hameleers, Michael, et al. "A Picture Paints a Thousand Lies? The Effects and Mechanisms of Multimodal Disinformation and Rebuttals Disseminated via Social Media." *Political Communication* 37, no. 2 (2020).

Ingram, Haroro J. *A Brief History of Propaganda during Conflict: Lessons for Counter-Terrorism Strategic Communications*. Netherlands: International Centre for Counter-Terrorism, 2016.

Jowett, Garth S., and Victoria O'Donnell. *Propaganda & Persuasion*. 6th ed. Newbury Park, CA: SAGE Publications, 2015.

Kersanskas, Vytautas. *Deterring Disinformation? Lessons from Lithuania's Countermeasures since 2014*, Hybrid Center of Excellence Paper 6. Helsinki: European Centre of Excellence for Countering Hybrid, Threats, 2021.