Prepared Statement
by
Testimony by Herbert Lin
Senior Research Scholar, Center for International Security and Cooperation
Hank J. Holland Fellow, Hoover Institution
Stanford University

Before the
House Armed Services Committee
Subcommittee on Cyber, Innovative Technology, and Information Systems
Hearing on
Technology and Information Warfare:
The Competition for Influence and the Department of
Defense

April 30, 2021

Chairman Langevin, Ranking Minority Member Stefanik, and distinguished members: thank you for calling today's hearing on technology and information warfare and for inviting me to testify today. I am speaking in my personal capacity and not on behalf of any institution with which I now or have ever had any affiliation. That said, I note that Stanford University receives a variety of grants, contracts, and other funding, including from DOD and other government agencies, that may touch on the subject matter of this hearing.

The general thrust of my remarks is that the Department of Defense is poorly authorized, structured, and equipped to cope with the information warfare threat facing the United States as a whole, although it can make meaningful contributions in addressing a portion of the problem.

Why is this so? The United States has no serious peer competitors in high-end, conventional conflict. But our adversaries know this fact and have learned to take advantage of a distinctly Western belief in a clear distinction between peace and war. It is true that we are not in a shooting war now with Russia or China, but we are not at peace either. Our adversaries prosecute this state of "not-peace" in many ways, including cyber-enabled information warfare.

On the Scope and Nature of the Cyber-Enabled Information Warfare Threat

I define information warfare as activities designed to convey to a target audience (whose size may be as small as a single individual or as large as a national population) information selected for their potential to influence emotions, motives, objective reasoning, attitudes, understanding, beliefs, or behavior in ways that advance the interests of the perpetrator.[1] (Note that in some cases, the intent or

[1] This list of desired effects is derived from both the current DOD definition of military support operations (Joint Publication 3-13.2, *Military Information Support Operations*, Washington, D.C. 2014, II-6.) and an earlier DOD

outcome may be to induce portions of the target audience to carry out subsequent activities to further the perpetrator's interests.[2]) Cyber-enabled information warfare is the conduct of information warfare that makes substantial use of modern information technologies, such as social media, search engines, artificial intelligence, and the Internet as well as traditional communications media technologies. (Note that the term "information warfare" is itself contested, as I mention below and I discuss in "Doctrinal Confusion and Cultural Dysfunction in DOD Regarding Information Operations, Cyber Operations, and Related Concepts," which I have submitted for the record.)

Cyber-enabled information warfare is a competitive and possibly hostile activity when conducted by an adversary against the United States or allies. But it is not warfare in any sense presently recognized under the laws of war or the United Nations Charter, and it is better characterized as adversarial psychological Internet-based manipulation of the target audience. Furthermore, the term is misleading in a DOD context, as the term "warfare" tends to connote a central role for the DOD. As I will address below, DOD is not well-positioned to address this threat comprehensively.

Cyber-enabled information warfare poses several new challenges. First, the Constitution of the United States is the foundation of U.S. government. Embedded deeply in the Constitution and especially in the First Amendment is the concept of a marketplace of ideas where the value of a specific idea is determined by the people in competition with other ideas rather than by the judgment of an external authority (such as government).[3] In this view, truth emerges through the public debate of ideas, uninhibited by governmental interference, and good ideas push out bad ideas.

Both U.S. political leaders and courts have invoked the marketplace metaphor. For example, Thomas Jefferson contended that "for here we are not afraid to follow truth wherever it may lead, nor to tolerate any error so long as reason is left free to combat it."[4] Nearly 150 years later, John F. Kennedy said "We are not afraid to entrust the American people with unpleasant facts, foreign ideas, alien philosophies, and competitive values. For a nation that is afraid to let its people judge the truth and falsehood in an open market is a nation that is afraid of its people."[5]

definition of psychological operations promulgated in 1984 (http://documents.theblackvault.com/documents/psyops/OvertPsyOps.pdf) as "planned political, economic, military, and ideological activities directed toward foreign countries, organizations, and individuals in order to create emotion, attitudes, understanding, beliefs, or behavior favorable to the achievement of U.S. political and military objectives." JP 3-13.2 Military Information Support Operations, 2011, page vii; also see JP3-13 Information Operations, 2014, II-9.

[2] Alicia Wanless and Michael Berk, "Participatory Propaganda: The Engagement of Audiences in the Spread of Persuasive Communications," in Proceedings of Social Media & Social Order, Culture Conflict 2.0, 1 December 2017, Oslo, https://www.researchgate.net/publication/329281610_Participatory_Propaganda_The_Engagement_of_Audiences_in_the_Spread_of_Persuasive_Communications.

[3] Much of this discussion is taken from Herbert Lin, "On the Organization of the U.S. Government for Responding to Adversarial Information Warfare and Influence Operations," *I/S: A Journal of Law and Policy for the Information Society* 15(1-2):1-43, Spring 2019.

[4] Thomas Jefferson, Letter to William Roscoe, 27 Dec. 1820, Web, https://www.loc.gov/exhibits/jefferson/75.html.

[5] John F. Kennedy: "Remarks on the 20th Anniversary of the Voice of America." February 26, 1962. Online by Gerhard Peters and John T. Woolley, *The American Presidency Project*. http://www.presidency.ucsb.edu/ws/?pid=9075.

As for the U.S. courts, Justice Oliver Wendell Holmes wrote in *Abrams v. United States* (1919) that "the ultimate good desired is better reached by free trade in ideas -- that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out.[6] Thirty-four years later, Justice William O. Douglas in *United States v. Rumely* explicitly introduced the term "marketplace of ideas" when he wrote "Like the publishers of newspapers, magazines, or books, this publisher bids for the minds of men in the market place of ideas."[7]

If we are to regard public discourse as a marketplace of ideas, a natural question arises: what happens when the market fails to promote better ideas and information of higher quality? Under what circumstances is intervention, government or otherwise, needed to remediate such failure? Justice Louis Brandeis' opinion in Whitney v. California (1927) points to the answer adopted by U.S. jurisprudence regarding the First Amendment. He wrote that

> "no danger flowing from speech can be deemed clear and present unless the incidence of the evil apprehended is so imminent that it may befall before there is opportunity for full discussion. If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence. Only an emergency can justify repression.[8]

Justice Brandeis' reasoning emphasizes "opportunity for full discussion" and time to "avert the evil by the processes of education" as key factors in judging whether intervention can be justified. Is the information environment of today one that provides such opportunity and time? Given that the advent of modern information technologies has brought with it a vast increase in the volume and velocity of information, it is clear that people cannot access all of the ideas and information that must be compared for sober reflection, and also that the time they have to do so has shrunk dramatically. The result is that people are able to process only a small fraction of the relevant information.

This leads to the second challenge. The information marketplace presumes that people process information rationally, thoughtfully, and deliberately. However, psychological science of the past 40+ years has demonstrated that people often do not do so. Instead, a variety of psychological factors shape the amounts and types of information to which they attend. Three of the most important factors are cognitive economy, dual-system cognition, and social identity. The impact of these factors on societal interaction, discourse, persuasion, and decision-making have been studied widely.[9]

[6] *Abrams v. United States*, 250 U.S. 616, 630 (1919)

[7] *United States v. Rumley,* 345 U.S. 45 (1953)

[8] Whitney v. California, 274 U.S. 357 (1927). https://supreme.justia.com/cases/federal/us/274/357/case.html.

[9] See, for example, Dan Ariely, *Predictably Irrational: The Hidden Forces That Shape Our Decisions*, Revised and expanded (New York, NY: Harper Perennial, 2010); Daniel Kahneman, Paul Slovic, and Amos Tversky, eds., *Judgment Under Uncertainty: Heuristics and Biases* (Cambridge: Cambridge University Press, 1982); Jonathan Baron, *Thinking and Deciding*, Fourth edition (Cambridge: Cambridge University Press, 2008); Robert B. Cialdini, *Influence: The Psychology of Persuasion*, Revised edition (New York, NY: Harper Business, 2006); Thomas Gilovich, Dale Griffin, and Daniel Kahneman, eds., *Heuristics and Biases: The Psychology of Intuitive Judgment* (Cambridge: Cambridge University Press, 2002).

- Cognitive economy refers to an inherently limited human cognitive-processing capability. For example, the number of unrelated items that human beings can remember for a short period of time is finite. Thus, when individuals are under time pressure to make decisions, they often select the first satisfactory solution rather than the optimal (best possible) one.[10] People can "use up" the resources needed for thoughtful and deliberate decision making; thus, their capability for such decision making in a limited time is restricted, and thus they tend to use thinking strategies that minimize the effort used in performing mental tasks so cognitive resources are conserved.[11]

- Dual-system cognitive theory posits the existence of some thinking strategies that operate at low cognitive cost and others that operate at higher cost. [12]

    - The low-cost system—often known as System 1—is fast, intuitive, reflexive, implicit, unconscious, "from the gut", and responsive to visual and other perceptual cues. It is based on principles (called heuristics) highly suited for making quick judgments and snap decisions.[13] Most important, System 1 thinking is the way human beings process information under most circumstances, and it is always operative (that is, it is never not functioning).
    - The higher-cost system—often known as System 2—is slower, more deliberate, analytical and consumes cognitive resources. Whereas System 1 thinking is mostly adequate to produce outcomes that are good enough for everyday use, System 2 thinking is generally more useful in considering situations involving complex inferences or deep understanding of nuance and subtlety. System 2 thinking involves a variety of thought processes associated

[10] The tendency to choose satisfactory solutions in favor of optimal ones is known as "satisficing" and was the subject of two papers by Herbert Simon ("A Behavioral Model of Rational Choice," *Quarterly Journal of Economics* 69 (1955): 99–118; "Rational Choice and the Structure of the Environment" *Psychological Review* (1956) 63: 129–138). The resulting theory of "bounded rationality" was the basis for Simon's 1978 Nobel Prize in Economics. Simon described the contrast between optimizing and satisficing as the difference between "looking for the sharpest needle in the haystack" (optimizing) and "looking for a needle sharp enough to sew with" (satisficing) (Simon H. A. "Satisficing." In *New Palgrave: A Dictionary of Economics*, Eatwell J, Millgate M, Newman P., eds., Vol. 4: Stockton Press: New York; 243–245, 1987). For an interesting example of decision making under extreme time pressure, see Hannah Oh, et al, "Satisficing in Split-Second Decision Making Is Characterized by Strategic Cue Discounting" (*Journal of Experimental Psychology*: Learning, Memory, and Cognition, 42(12):1937-1956, 2016, https://doi-org.stanford.idm.oclc.org/10.1037/xlm0000284.)

[11] See, for example, Susan T. Fiske and Shelley E. Taylor, *Social Cognition* (Reading, MA: Addison-Wesley Pub. Co., 1984).

[12] For a primer on System 1 and System 2 thinking, see Daniel Kahneman, *Thinking, Fast and Slow* (Farrar, Straus and Giroux, 2011); and see also the discussion of Type 1 (*i.e.*, System 1) and Type 2 (*i.e.*, System 2) thinking in Keith E. Stanovich, *What Intelligence Tests Miss: The Psychology of Rational Thought* (Yale University Press, 2009). For other variants of dual-system cognitive theory, see Richard E. Petty and John T. Cacioppo, "The Elaboration Likelihood Model of Persuasion," in *Advances in Experimental Social Psychology*, ed. Leonard Berkowitz, vol. 19 (Academic Press, 1986), 123–205, https://doi.org/10.1016/S0065-2601(08)60214-2; and Shelly Chaiken, "The Heuristic Model of Persuasion," in *Social Influence: The Ontario Symposium, Vol. 5.*, Ontario Symposium on Personality and Social Psychology (Hillsdale, NJ, US: Lawrence Erlbaum Associates, Inc, 1987), 3–39.

[13] Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science* 185, no. 4157 (September 27, 1974): 1124–31, https://doi.org/10.1126/science.185.4157.1124.

with formal logic, reasoning and rationality, symbolic abstraction, serial rule-based processing, and language and conscious thought.

Reliance on System 1 thinking is not a tendency limited to less educated or less intelligent individuals. All people—regardless of level of education, intelligence, profession, or political persuasion—rely on such thinking to some degree to their detriment under some circumstances.

- Social (or group) identity is important to most individuals. Groups form on the basis of similarities such as ethnicity, gender, age, religion, social class, employment status, geography, political party, personal beliefs, values, attitudes, aspirations, moral values, recreational activities, attitudes toward sexual activity. People in groups are highly motivated to establish a shared reality (including shared attitudes, feelings, and emotions) to validate their identity and experiences.[14] Group identity can be threatened by information that casts doubt on any important aspect of a group's shared reality, and people often respond by rejecting, ignoring, disbelieving, or discrediting such information or by finding error in it regardless of its objective truth. A consequence is what has been described as motivated reasoning,[15] which refers to a person's desire to reach a particular conclusion. When engaged in motivated reasoning, people choose a selective set of cognitive processes for strategies for accessing, constructing, and evaluating beliefs, and they search their memory for beliefs, rules, and knowledge to support the conclusions required for maintenance of their group identity.

Propagandists have understood these insights from the psychology of human cognition for millennia. However, in the past half-century, psychological science has produced thousands of peer reviewed empirical studies that have begun to formalize this understanding. The psychology human cognition has revolutionized the study of economics, where assumptions of rationality have been replaced by recognition of serious biases and non-rational thinking. The result—behavioral economics—has led to three Nobel Prizes being awarded to leaders in the field: Herbert Simon, Daniel Kahneman, and Richard Thaler.

These psychological insights also inform the behavior of the technology companies that have built today's information environment. Private companies—including the tech companies—exist to make money, and making money through cyberspace is only possible through two mechanisms: charging a monetary fee for some technology-related service or selling advertisements to users of that service. To date, no other sustainable business models have been developed.

Many large platform and media companies depend on selling advertisements to lower or eliminate the payment of monetary fees. They thus depend on users being willing to pay attention to their ads, which in turn requires them to maximize the time users spend using their services—that is, to maximize user engagement. These companies have learned that maximizing user engagement is easiest when they provide customized content and activities to individual or small groups of users. It turns out that a computer-based analysis of an individual's digital footprint (e.g., as expressed by the person's

[14] Michael A Hogg and Mark J Rinella, "Social Identities and Shared Realities," *Current Opinion in Psychology*, Shared Reality, 23 (October 1, 2018): 6–10, https://doi.org/10.1016/j.copsyc.2017.10.003.

[15] See, for example, Ziva Kunda, "The Case for Motivated Reasoning," *Psychological Bulletin* 108, no. 3 (1990): 480–98, https://doi.org/10.1037/0033-2909.108.3.480.

pattern of "likes") can be more accurate than those made by friends and even spouses in predicting matters such as substance use, political attitudes, and physical health.[16]

The psychology of cognition is important because knowledge of an individual's psychological profile enables companies to provide content that plays to the worst habits of System 1 thinking. For example, System 1 thinking drives people to seek novel information, regardless of its veracity. An important study in Science examining the spread of information on Twitter found that false information couched as news spread much more widely and more rapidly than true information, suggesting that the degree of novelty and the emotional reactions of recipients could be responsible for the differences observed.[17] The motivation of companies for providing such content is not partisan but rather revenue-driven, and if it happens that users are more likely to be driven into more extreme political positions, that is merely a side effect of their business model.

The third challenge is that the boundaries between foreign and domestic sources of information chaos and dysfunction are blurring. It may or may not be true that certain Russians and Americans work together in smoky conference rooms to actively plan out a cyber-enabled IW campaign against the United States to sow disorder, mistrust, and polarization—but the scope, nature, and effects of their activities, even if separately conducted, are largely indistinguishable. This means that effective efforts against the Russian activities will inevitably have collateral effects against American activities that are similarly oriented.

For example, Russian media have devoted considerable attention to the allegations of a single U.S. blogger who asserted that Antifa was responsible for provoking the siege of the Capitol on January 6, 2021.[18] These stories echoed similar allegations aired on the Rush Limbaugh show on the day of the siege, which cited former FEMA director Michael Brown claiming that Antifa supporters were breaching security at the Capitol.[19] Both narratives—those from Russian media and from the Limbaugh show share important characteristics. First, they are thinly sourced. Second, neither Russian nor American outlets take responsibility for the content of the allegations—they are "merely" reporting on what someone else said or on rumors circulating in the information ether. Third, and most important, neither provide any evidence to support the underlying claim (nor has any evidence surfaced since then to indicate the truth of the claim). Nevertheless, these narratives have achieved considerable prominence in certain segments of the American populace.[20]

[16] Wu Youyou, Michal Kosinski, and David Stillwell, "Computer-Based Personality Judgments Are More Accurate than Those Made by Humans," *Proceedings of the National Academy of Sciences* 112(4):1036-1040, https://doi.org/10.1073/pnas.1418680112.

[17] Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online." *Science* 359(6380):1146-1151, March 9, 2018, https://doi.org/10.1126/science.aap9559.

[18] See, for example, "Очевидец: Штурм Капитолия Спровоцировали Члены 'Антифа.'" ("Eyewitness: Antifa members provoked the storming of the Capitol"), vesti.ru, January 12, 2021, https://www.vesti.ru/article/2509238; and "Штурм Капитолия членами 'Антифа'", ("The storming of the Capitol by members of 'Antifa'"), *60 minutes*, smotrim.ru, January 12, 2021, https://smotrim.ru/video/2258111.

[19] https://www.happyscribe.com/public/the-rush-limbaugh-show/the-rush-limbaugh-show-podcast-jan-06-2021, transcript at the 01:14:27 time mark.

[20] https://www.usatoday.com/story/news/politics/2021/02/21/exclusive-trump-party-he-still-holds-loyalty-gop-voters/6765406002/

I know of no claim from anyone that the Russian government was behind the Capitol siege—if it were, one could argue that the U.S. government would have an important role in responding to such involvement. One could even argue, though less plausibly, that the U.S. government should take action against Russian media outlets engaging in scurrilous reporting that damages U.S. interests. But it is entirely clear any domestic action to suppress the claim of Antifa provocation of or involvement in the Capitol siege would be inconsistent with First Amendment jurisprudence, even if such a claim is false.

A second and related example is that about 20 percent of Facebook postings in 2020 and early 2021 relating to QAnon originated outside the United States, with China and Russia playing leading roles in this activity. During 2020, posts originating in Russia accounted for 44 percent, while in early 2021, posts originating in China accounted for 58 percent of such posts.[21] That leaves many other posts, however, and undoubtedly some originate from domestic sources with First Amendment and other constitutional protections.

A third example is provided by the National Intelligence Council,[22] which assessed with high confidence that "a range of Russian government organizations conducted information warfare operations aimed at denigrating President Biden's candidacy and the Democratic Party, supporting former President Trump, undermining public confidence in the electoral process, and exacerbating sociopolitical divisions in the US," noting that "a key element of Moscow's strategy this election cycle was its use of proxies linked to Russian intelligence to push influence narratives—including misleading or unsubstantiated allegations against President Biden—to U.S. media organizations, U.S. officials, and prominent U.S. individuals, including some close to former President Trump and his administration." U.S. parties pushing Russian narratives, even unwittingly, are afforded much greater protection against government interference with their activities than would Russians be in pushing those same narratives.

In sum, the information warfare threat to the United States is different from other threats that the nation has faced in the past. Our information warfare adversaries have weaponized our constitutional protections, our minds, and our technologies against us. Cyber-enabled information warfare has the potential to destroy reason and reality as the basis for societal discourse and to replace them with rage and fantasy. In the long run, perpetual civil war and political extremism, waged in the information sphere and egged on by our adversaries, is every bit as much an existential threat to American civilization and democracy as any military threat imaginable.[23]

Misalignment Between the Department of Defense and the Information Warfare Threat

Why can't DOD defend the United States against the information warfare threat? At the highest level of abstraction, the reason is that the information warfare threat requires not only a whole-of-

[21] The Soufan Center, "Quantifying The Q Conspiracy: A Data-Driven Approach to Understanding the Threat Posed by QAnon," April 2021, https://thesoufancenter.org/research/quantifying-the-q-conspiracy-a-data-driven-approach-to-understanding-the-threat-posed-by-qanon/.

[22] National Intelligence Council, Foreign Threats to the 2020 U.S. Federal Elections, ICA-2020-00078D, March 15, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

[23] Herbert Lin, "The existential threat from cyber-enabled information warfare," *Bulletin of the Atomic Scientists*, 75(4):187-196, 2019, DOI: 10.1080/00963402.2019.1629574.

government response but rather a whole-of-society response, and DOD—as broad as its legal purview is—cannot orchestrate either one.

More specifically, the answer is that DOD is constrained by policy and by culture from doing so effectively.[24]

DOD Directive 3600.01 governs DOD information operations within the United States: "DOD IO activities will not be directed at or intended to manipulate audiences, public actions, or opinions in the United States and will be conducted in accordance with all applicable U.S. statutes, codes, and laws."[25] This restriction would seem to prohibit DOD activities directed at U.S. audiences, regardless of the intent underlying those activities, and in particular activities to protect U.S. audiences against foreign information warfare operations.

The directive does not cite a statutory basis for this restriction. However, in 2009, Public Law 111-84 changed the U.S. Code (in 10 U.S. Code § 2241a) to prohibit the expenditure or obligation of DOD funds for publicity or propaganda purposes within the United States not otherwise specifically authorized by law.[26] At the same time, most people when queried believe that the Smith-Mundt Act of 1948 (Public Law 80-402) is the basis for this DOD directive, even though the text of the Smith-Mundt Act is irrelevant to DOD operations.

The cultural constraints within the DOD loom large as well. They start from the observation that the threat is informational rather than physical. Despite rhetoric and doctrinal statements to the contrary, U.S. military culture is oriented towards the physical world and the operational environment. It has historically looked to the operational environment as where battles are won. Mass, firepower, and technological overmatch have been regarded as the tools with which to win battles, and physical engagement, courage, and bravery are honored above other personal attributes in soldiers. It is thus not entirely surprising that some do not view soldiers with non-kinetic specialties with the same respect as they do for combat arms troops with specializations in more traditional fields such as infantry, armor, and artillery. Indeed, soldiers specializing in information operations—and especially psychological operations—often report feeling that others regard them with disdain and even contempt.

DOD joint doctrine does not explicitly acknowledge the possibility that U.S. audiences (or armed forces) could be the target of adversary psychological operations to influence the emotions, motives, objective reasoning, and behavior of U.S. forces. By contrast, definitions of many other DOD operations do incorporate the idea that U.S. forces conduct operations to compromise adversary functions while protecting the same functions for U.S. forces.

Matters are further complicated by the fact that psychological operations have been singled out for some negative comparisons even among the non-kinetic combat capabilities. For example, In 2011, the term "psychological operations" (PSYOP) was superseded by "military information support

[24] Much of this discussion is taken from Herbert Lin, "Doctrinal Confusion and Cultural Dysfunction in DOD Regarding Information Operations," Cyber Operations, and Related Concepts, *Cyber Defense Review*, Summer 2020.

[25] DOD Directive 3600.01 Information Operations, Undersecretary of Defense for Policy, May 2, 2013 Incorporating Change 1, May 4, 2017, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODD/360001p.pdf

[26] https://www.law.cornell.edu/uscode/text/10/2241a.

operations," on the directive of then-SECDEF Robert Gates, whose explanation for the name change was that "although psyop activities rely on truthful information, credibly conveyed, the term PSYOP tends to connote propaganda, brainwashing, manipulation, and deceit."[27] Furthermore, the conduct of psychological operations often require higher authorities than for kinetic operations. For example, during Operation INHERENT RESOLVE, the authority to strike ISIS kinetically required a brigadier general or even below, while an information operation—including a psychological or military information support operation—required the approval of a at least a major general. Indeed, at the start of INHERENT RESOLVE, some such operations required approval at the level of the National Security Council. Any such operation conducted via the Internet or social media required Pentagon-level approval.[28] These constraints have led to an often-expressed sentiment that "it is easier to get permission to kill terrorists than it is to lie to them."

DOD organization for psychological operations reflects these attitudes. The vast majority of DOD psychological operations personnel are Army, and most of these Army personnel are under the operational command of the Army Public Affairs and Psychological Operations Command,[29] which itself is an Army reserve command. Only a relatively small fraction of Army psychological operations personnel are active-duty soldiers, a point that might suggest that the expertise of these personnel is regarded as less important in military operations that are carried out by those on active duty. Psychological operations personnel are also generally qualified special forces operators under the operational command of USSOCOM, where they undoubtedly benefit from the elite status of being such operators and likely helps to offset any stigma associated with psychological operations.

Finally, DOD terminology and doctrine as understood by troops in the field are confused and inconsistent on the meaning of important terms such as information warfare, information operations, cyber operations, psychological operations/military information support operations, and information warfare operations. Nowhere is this better seen than in advocacy that cyber forces expand their ambit to include information operations and information warfare.

For example, *Army Times* reported in late 2019 that U.S. Army Cyber Command was proposing to change its name to Army Information Warfare Command,[30] quoting Lt. Gen. Stephen Fogarty, Commander, U.S. Army Cyber Command, as saying "Sometimes, the best thing I can do on the cyber side is actually to deliver content, deliver a message. ... Maybe the cyberspace operation I'm going to conduct actually creates some type of [information operation] effect." In this context, it is clear that as in many other instances, the term "information operations" is being used as a virtual synonym for psychological operations.

[27] U.S. Marine Corps, "Changing The Term Psychological Operations to Military Information Support Operations" (Washington D.C.: U.S. Marine Corps, December 12, 2011), https://www.marines.mil/News/Messages/MARADMINS/Article/887791/changing-the-term-psychological-operations-to-military-information-support-oper/.

[28] Cole Livieratos, "Bombs, Not Broadcasts", *Joint Forces Quarterly*, Number 90, pp. 60-67, 3rd Quarter 2018, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-90/jfq-90.pdf.

[29] "About Us: U.S. Army Civil Affairs & Psychological Operations Command (Airborne)" (Fort Bragg, NC: U.S. Army Reserve), https://www.usar.army.mil/Commands/Functional/USACAPOC/About-Us/.

[30] Kyle Rempfer, "Army Cyber Lobbies for Name Change This Year, as Information Warfare Grows in Importance," *Army Times*, October 16, 2019, https://www.armytimes.com/news/your-army/2019/10/16/ausa-army-cyber-lobbies-for-name-change-this-year-as-information-warfare-grows-in-importance/.

A similar story applies to the 16th Air Force. Prior to its creation in October 2019, one press report noted a senior Air Force official saying that the new organization [that is, the organization that would become the 16th Air Force] will focus on "cyber information operations, influence operations, electronic warfare, military deception, military information support operations and psychological operations."[31] The site is replete with references to "cyber," and the commander of the 16th Air Force has a background that is squarely in the cyber domain as the commander of the cyber National Mission Force. However, in late February 2020, a search of the 16th Air Force web site for "military information support operations" turned up zero references. The word "psychological" yielded one reference—a reference to a component of 16th Air Force (the 480th ISR Wing) that conducted psychological operations in 1952 and was subsequently deactivated in 1953. The site contains many references to "information operations," but examination of these references suggests no connection to psychological operations or military information support operations.

The strongly technical emphasis and history of the DOD cyber warfare community causes me to question whether DOD is well-positioned to embrace and integrate the psychological aspects of information operations.[32] Various service cyber commands (including U.S. Cyber Command) have appropriately concentrated on acquiring the technical expertise that cyberspace operations require, but the expertise needed to conduct psychological operations goes beyond the skill set of cyber operators. Nor do the various cyber commands appear particularly interested in obtaining such expertise—a keyword search on USAJOBS (conducted on April 28, 2021) for jobs involving "cyber" and "psychology" or "cyber" and "psychological" turned up one job for an instructional systems specialist unrelated to operations. A keyword search on "cyber command" yielded 87 job listings, with many openings for information technology or cybersecurity specialists and zero openings asking for any expertise remotely connected to psychology.

What is the Appropriate Role for the Department of Defense in Addressing the Information Warfare Threat?

The DOD can pursue offensive and defensive activities with respect to information warfare, but it must be realized that offensive activities will not help to defend the U.S. population against the information warfare threat. Moreover, since our information warfare adversaries are authoritarian entities, they already exercise a great deal of control and influence over the information that flows through their borders or into their spheres of influence. Thus, offensive information warfare activities of the United States would be pitted against a strong suit of authoritarian governments.

Nevertheless, should the DOD wish to prosecute the offensive side of information warfare against foreign adversaries, I begin with the observation that the DOD cyber operators appear to be expanding their purview into the information warfare space. However, the expertise of DOD cyber forces to this point in time has focused on the information *delivery* side of cyber-enabled psychological operations. Prosecuting information warfare requires content as well, and it is by virtue of long

[31] Mark Pomerleau, "Air Force Hopes New Organization Can Boost Electronic Warfare," *C4ISRNET*, April 15, 2019, https://www.c4isrnet.com/electronic-warfare/2019/04/15/air-force-hopes-new-organization-can-boost-electronic-warfare/.

[32] The discussion here focuses on the psychological aspects. The same may well be true for other facets of information operations.

experience in executing influence operations that U.S. Special Operations Command has developed its extensive psychological and cultural expertise on the information *content* side of psychological operations.

Thus, DOD should establish a standing operational entity that can integrate specialists in psychological operations and in cyber operations as co-equal partners. This entity would bring "to bear the respective expertise of each command [Cyber Command for cyber expertise, Special Operations Command for psychological operations] should . . . enhance the synergies possible between cyber-enabled psychological operations and offensive cyber operations, and it would be most desirable if the two commands could partner rather than compete over the cyber-enabled psychological operations mission."[33] The "standing" part of this entity is essential, as it would recognize the continuing need to conduct such operations against adversaries who believe that open conflict need not have been declared or even started for hostile activity in information space to begin.

Perhaps the most important policy matter in pursuing the offensive side of information warfare is the extent to which DOD offensive information warfare operations are constrained by a need to be truthful and not misleading. A long tradition of U.S. efforts in this regard, especially those undertaken during the Cold War, reflects a deeply-held belief that as long as the United States presents truthful information against adversaries that lie and mislead, it will prevail. But the Cold War ended before the advent of the Internet, social media, search engines and other information technologies that have changed the information environment by many orders of magnitude. The very successes of our information warfare adversaries today have demonstrated that truth does not always prevail, in part because lies spread faster than truth and because the first message to get through has significant advantages. What may have been true about likely winners and losers in the past may not be so true today and in the future.

How and to what extent, if any, should the United States and DOD adopt the tactical approaches of our information warfare adversaries against them is an open question. As an American citizen, I am very uneasy with the idea of my government using deception and misdirection as tools of its defense and foreign policy, and yet I wonder if relying only on truths that move at a snail's pace in cyberspace leaves us at a fundamental disadvantage with respect to our adversaries. Sometimes we do accept disadvantage as a matter of principle—it is our stated policy to adhere to the laws of armed conflict whether or not our adversaries so. But the ethics of how to conduct information warfare ourselves is perhaps a different issue that is way above my pay grade to address.

Addressing the defensive side of information warfare conducted against the populace of the United States is also complex. DOD's freedom of action is constrained by policy and public concerns about DOD actions that directly affect the information available to U.S. citizens. Nevertheless, DOD is well positioned to address the cyber-enabled information warfare threat for at least one important segment of the U.S. populace—the U.S. armed forces and their families. Consider that:

- Every member of the U.S. military swears an oath to "support and defend the Constitution of the United States against all enemies, foreign and domestic." But DOD offers essentially zero training on what it means in a practical or operational sense to "support and defend" the Constitution and how to identify an "enemy, foreign or domestic."

[33] https://www.lawfareblog.com/integration-psychological-operations-cyber-operations.

- Section 589E of the FY2021 National Defense Authorization Act called for the DOD to establish a training program regarding foreign malign influence campaigns for U.S. military personnel and their families.[34] Although the legislation provided no specifics on the content of the training program, it is hard to imagine that it would not try to teach/educate U.S. military personnel how to identify and resist the influence of hostile information warfare campaigns.

- Section 589F of the FY2021 National Defense Authorization Act called for DOD to assess aspects of the foreign information warfare threat to members of the U.S. armed forces and their families,[35] although the legislative language used somewhat different terms than are used in this testimony.

- Secretary of Defense Austin has taken action to counter extremism in the Department of Defense, including the military personnel within DOD.[36] The scope, nature, and extent of extremism within the U.S. armed forces is unknown at this time, and Secretary Austin's actions will shed some light on these matters. Nevertheless, to the extent that extremism is a problem, it is clear that information warfare operations and exposure to disinformation contribute in some ways to the problem.

Taken together, these points suggest that DOD does have the legal and moral authority--indeed, I would suggest the responsibility—to take action to defend the U.S. armed forces and their families against the foreign information warfare threat.

I further observe the importance of the ongoing bipartisan effort to promote civics education through a grants and fellowship program that would be run by the Department of Education (H.R. 1814). That legislation does not touch the Department of Defense, nor should it, but it should be obvious that a foundation in civics education is an essential pre-requisite for understanding the Constitution that members of the armed forces have sworn to support and defend. Moreover, ignorance about civics and the Constitution has apparently been a major contributor to the political and societal dysfunction that we have all witnessed in the last several months. Again, it should be clear that such dysfunction only plays into the hands of our authoritarian adversaries, who fan the flames of discontent and point to their comparatively calm and orderly societies in contrast. A better illustration of non-military national security threats could not be imagined.[37]

[34] https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf

[35] https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf

[36] https://www.defense.gov/Newsroom/Releases/Release/Article/2567545/secretary-of-defense-austin-announces-immediate-actions-to-counter-extremism-in/

[37] The Center for Strategic and International Studies has underway a project entitled "Civics as a National Security Imperative" (https://www.csis.org/programs/international-security-program/civics-national-security-imperative) that seeks to reinvigorate and prioritize civics and civic education as an essential part of U.S. national security. According to the website, the project focuses on "the opportunity and imperative to rediscover our shared values, relearn the fundamentals of our constitutional republic, and re-form a sense of civic identity and commitment in our communities and across the nation."

Accordingly, DOD should:

- Acknowledge in doctrine the vulnerabilities of its personnel to information warfare operations and the importance of protecting its personnel against such operations and allocate the necessary resources to build capacity and broad understanding as indicated below.

- Augment its basic training and professional military education requirements to include instruction on the meaning of "defending the Constitution against all enemies, foreign and domestic." These should be conducted at least at the same intensity and level (preferably higher) as the instruction that uniformed DOD personnel receive regarding compliance with the laws of armed conflict. The proper content of such instruction remains to be determined, but an example could be instruction on the appropriate response of a service member who observes other service members engaged in activities that could constitute violations of their oaths.

- Support civics education for both the members of the armed forces (perhaps as part of instruction on defending the Constitution), their families, and also for the broader public. (The DOD Educational Activity schools educate over 70,000 children of service members, and is a wonderful place to spearhead the development of civics education curricula.) A guiding precedent for supporting civics education could well be the National Defense Education Act of 1958 that sought to increase support for science and mathematics education in the wake of the national security threat posed by what appeared to be rapidly advancing Soviet science in light of the launch of Sputnik. Now, we face a second 'Sputnik moment' and a need to re-invigorate civic education in the population at large. What better place to start than with the members of our military services and their families?

As noted earlier, DOD is not in a position to lead a whole-of-society defense against to the information warfare threat. But it can and should take point in defending its service members and their families, recognizing that such efforts may well provide a model for other parts of society to follow in its footsteps.

I will be happy to answer any questions from the committee.

Attachments for the record

- Herbert Lin, "The Existential Threat from Cyber-Enabled Information Warfare," *Bulletin of the Atomic Scientists* 75(4):187-196, July 2019.

- Herbert Lin, "On the Organization of the U.S. Government for Responding to Adversarial Information Warfare and Influence Operations," *I/S: A Journal of Law and Policy for the Information Society* 15(1-2):1-43, Spring 2019.

- Herbert Lin, "Doctrinal Confusion and Cultural Dysfunction in DOD Regarding Information Operations," Cyber Operations, and Related Concepts, *Cyber Defense Review*, Summer 2020.