[H.A.S.C. No. 117–25]

TECHNOLOGY AND INFORMATION WARFARE: THE COMPETITION FOR INFLUENCE AND THE DEPARTMENT OF DEFENSE

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

HEARING HELD
APRIL 30, 2021

U.S. GOVERNMENT PUBLISHING OFFICE
44–945 WASHINGTON : 2021

SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

JAMES R. LANGEVIN, Rhode Island, *Chairman*

RICK LARSEN, Washington
SETH MOULTON, Massachusetts
RO KHANNA, California
WILLIAM R. KEATING, Massachusetts
ANDY KIM, New Jersey
CHRISSY HOULAHAN, Pennsylvania, *Vice Chair*
JASON CROW, Colorado
ELISSA SLOTKIN, Michigan
VERONICA ESCOBAR, Texas
JOSEPH D. MORELLE, New York

JIM BANKS, Indiana
ELISE M. STEFANIK, New York
MO BROOKS, Alabama
MATT GAETZ, Florida
MIKE JOHNSON, Louisiana
STEPHANIE I. BICE, Oklahoma
C. SCOTT FRANKLIN, Florida
BLAKE D. MOORE, Utah
PAT FALLON, Texas

TROY NIENBERG, *Counsel*
CHRIS VIESON, *Professional Staff Member*
CAROLINE KEHRLI, *Clerk*

CONTENTS

TECHNOLOGY AND INFORMATION WARFARE: THE COMPETITION FOR INFLUENCE AND THE DEPARTMENT OF DEFENSE

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS,
Washington, DC, Friday, April 30, 2021.

The subcommittee met, pursuant to call, at 3:04 p.m., via Webex, Hon. James R. Langevin (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, CHAIRMAN, SUBCOMMITTEEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

Mr. LANGEVIN. Good afternoon, everyone. The subcommittee will come to order. First of all, just some housekeeping business that I need to take care of, since this is a remote hearing.

I would like to welcome the members who are joining today's remote hearing, which, I believe, is just about everybody.

Members who are joining must be visible onscreen for the purposes of identity verification, establishing and maintaining a quorum, participating in the proceeding, and voting. Those members must continue to use the software platform's video function while in attendance unless they experience connectivity issues or other technical problems that render them unable to participate on camera.

If a member experiences technical difficulties, they should contact the committee staff for assistance.

A video of members' participation will be broadcast via the television internet feeds.

Members participating remotely must seek recognition verbally, and they are asked to mute their microphones when they are not speaking.

Members who are participating remotely are reminded to keep the software platform's video function on the entire time they attend the proceeding.

Members may leave and rejoin the proceeding. If members depart for a short while for reasons other than joining a different proceeding, they should leave the video function on.

If members will be absent for a significant period or depart to join a different proceeding, they should exit the software platform entirely, and then rejoin if they return.

Members may use the software platform's chat feature to communicate with staff regarding technical or logistical support issues only.

Finally, I have designated a committee staff member to, if necessary, mute unrecognized members' microphones to cancel any inadvertent background noise that may disrupt the proceeding.

So with the technical announcements out of the way, I am just going to now give my opening statement.

First of all, I want to say welcome to our hearing today on the Technology and Information Warfare: The Competition for Influence and the Department of Defense. I want to thank Ranking Member Stefanik for joining me in holding the hearing today.

I would also like to thank our witnesses for appearing today. To discuss technology-enabled information warfare as a national security threat, we welcome Mr. Glenn Gerstell, senior adviser at the Center for Strategic and International Studies, and Ms. Nina Jankowicz, disinformation fellow at the Wilson Center. And to provide insight on the Pentagon's information operation strategy and leadership, we are joined by Dr. Herb Lin, senior research scholar at Stanford University. And finally, Dr. Joseph "Joe" Kirschbaum, Director, Defense Capabilities and Management Team at the Government Accountability Office.

First of all, I want to say, Dr. Kirschbaum, welcome back, and I want to thank you all for appearing today. It is an honor to have you here, and truly it is an esteemed panel.

So, the United States is challenged in the information environment daily. Competitors like China, Russia, and violent extremist organizations use information warfare to achieve their objectives, while—below the threshold of armed conflict, as they seek to avoid traditional U.S. military advantages, and undermine the free international order and democratic values.

The recently released Annual Threat Assessment of the U.S. intelligence community makes clear that a variety of state and nonstate actors weaponize information to undermine the United States by sowing discord among our citizens, influencing decision makers, and reversing what had once been a strength of our Nation's historical information advantage.

So, I often focus on what lies ahead in defense, but it is worth noting that the United States and the military are facing momentous challenges in the information environment right now, which can undermine the very fabric of our democracy.

And what makes these threats particularly powerful is that foreign adversaries can target U.S. and allied citizens almost instantly without crossing physical boundaries or borders. These threats will only grow as artificial intelligence, machine learning, and other technology-enabled information operations exponentially increase the speed and the scope of the danger.

So according to the National Security Commission on Artificial Intelligence, state adversaries are employing artificial intelligence-enabled disinformation attacks to sow division in democracies and disrupt the public's sense of reality.

But how to confront these national security challenges is a difficult question. So I believe the Nation must respond forcefully to deter bad actors in the information domain, invest in robust U.S.

public diplomacy, and educate the public and our service members about these dangers.

We must also articulate a vision for the information environment and delineate thresholds of behavior that will trigger a response.

So I was sort of encouraged when the National Security Commission on Artificial Intelligence recommended that the United States develop a new strategy to counter disinformation while investing in technology to counter artificial intelligence-enabled information warfare.

And I am also looking forward to the insight our witnesses will provide on how to address these threats.

Likewise, we will explore how the Department of Defense is organized to compete in the information environment, including cyber, electromagnetic spectrum, military information support operations, deception, and operational security.

The military is challenged, in the information environment, by capable adversaries—make no mistake about it—and Department of Defense priorities must reflect this reality. The Pentagon has a critical role in protecting the Nation, our partners, and our allies from threats in the information environment, and in advancing our national interests in this sphere.

Recognizing this, Congress and this committee have continuously pushed the Department to prioritize adapting to the weaponized information environment, including by creating the principal information operations adviser.

Yet, I am concerned the Department leadership has been slow to adapt to the changing nature of warfare in this domain. To give an example, in 2020, 9 of the then 11 four-star combatant commanders wrote a memorandum asking for additional support for their information operations.

They wrote, and I quote, "We continue to miss opportunities to clarify truth, counter distortions, puncture false narratives, and influence events in time to make a difference," close quote.

I couldn't agree more. Too often, it appears, the Department's information-related capabilities are stovepiped centers of excellence with varied management and leadership structures which makes critical coordination more difficult.

Further, the Pentagon has made limited progress implementing the 2016 Operations in the Information Environment Strategy, which raises questions about the Department's information operations leadership structure.

So with that, these are challenging questions without easy answers, I know that. But I hope my colleagues will take advantage of the impressive array of witnesses that we have before us to get a little clarity and a clear path forward after this hearing.

So with that, I will now turn to Ranking Member Stefanik for her opening remarks. Elise, you are recognized.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 31.]

STATEMENT OF HON. ELISE M. STEFANIK, A REPRESENTATIVE FROM NEW YORK, RANKING MEMBER, SUBCOMMITTEE ON CYBER, INNOVATIVE TECHNOLOGIES, AND INFORMATION SYSTEMS

Ms. STEFANIK. Thank you, Chairman Langevin, and thank you to our witnesses for testifying today. Information warfare is one of the most complex and important missions undertaken by the Department of Defense, especially in the 21st century information age.

From large-scale, conventional conflicts of the past to the modern-day, gray-zone conflicts of today, information operations have been critical to shaping the operating environment and weakening our adversaries' strategic position.

Eroding the resilience of our target adversaries, while also winning the hearts and minds, remains the ultimate objective of information operations. As a former senior adviser to the Secretary of Defense, Robert Riley, said, quote, "Ultimate victory comes when the enemy speaks your language, and embraces your idea," end quote.

Unfortunately, we know our adversaries are not embracing our ideas. Instead, China, Russia, Iran, and non-state actors alike, are weaponizing information to undermine the United States and our interests, employing asymmetric information capabilities, rather than engaging us in traditional military means.

Therefore, we must be prepared to not just resist information operations and defend our interests, but also project our own capabilities to exploit and shape the information environment.

Today's information and media ecosystem is significantly different than the past, with exponential advancements in technology allowing words and ideas to spread faster and wider than ever before.

In the last decade, we have seen how a short video, photo, or social media post, can have a profound impact on the geopolitical landscape.

Going forward, international competition, diplomacy, and military operations will be increasingly based on human-centric networks and patterns. Fortunately, our military and intelligence community recognize this, and both are adapting to this landscape and the information in which we live.

Congress has given clear authorities to DOD [Department of Defense] to conduct information operations, and we expect the Department to use those authorities effectively. As such, we can no longer just rely solely on our special operations forces to conduct these operations. This must be a comprehensive approach by the DOD, the services, and combatant commands, to ensure our messages are effective in achieving our objective to positively shape the operating environment.

Two years ago, Congress required the Department to conduct a review of its information operation strategy. However, we are still awaiting this review and briefing.

This subcommittee, in particular, with jurisdiction over cyber and artificial intelligence, is uniquely suited to support the Department's information operations. Yet without the proper review and information from DOD, it is difficult to appropriately support this priority.

Congress has also created the position of the principal information operations adviser, so the Department would have a single person overseeing military information support operations, or MISO, efforts.

Unfortunately, this position was layered below the Under Secretary of Defense for Policy, contrary to congressional intent. This position was not created as another bureaucratic layer, but as an agile single role with the mandate to guide each service's efforts.

We must also act on the recommendations from the AI [artificial intelligence] commission and invest in technologies to combat AI-enabled information threats, as well as increase coordination with the State Department's Global Engagement Center to counter foreign propaganda targeted towards the United States.

I look forward to hearing from our witnesses on how DOD can organize information operations to be more coherent, nimble, agile, and effective, and how the Department and the IC [intelligence community] can work together to enhance MISO efforts.

Likewise, we must continue to discuss the critical defensive roles DOD can play to protect the information environment as our adversaries continue to wage a persistent information war on our interests abroad, and our citizens here at home.

Thank you, Mr. Chairman, and I yield back.

Mr. LANGEVIN. Thank you, Ranking Member Stefanik.

With that, I will now turn to our witnesses. We will now hear from Mr. Glenn Gerstell. Mr. Gerstell served as the National Security Agency general counsel from 2015 to 2020, is now a senior adviser at the Center for Strategic and International Studies.

Mr. Gerstell, you are now recognized to summarize your testimony for 5 minutes, and thank you for appearing today.

STATEMENT OF GLENN S. GERSTELL, SENIOR ADVISER, INTERNATIONAL SECURITY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Mr. GERSTELL. Chairman Langevin, Ranking Member Stefanik, and members of the subcommittee, thank you for the opportunity to appear before you today along with such distinguished experts.

Over the past few months, social media platforms have been awash in falsehoods on political topics ranging from election fraud, to the Capitol insurrection, to climate change and Antifa protestors.

Even the seemingly non-partisan sphere of public health has been politicized and damaged by cyber falsehoods about the efficacy of face masks and vaccinations.

As a former national security official and a lawyer concerned with our civil liberties, I would offer three observations relevant to the subcommittee's work.

First, perhaps the most pernicious aspect of the digital revolution, disinformation, intentionally misleading, erroneous information threatens our very democracy, leading to mistrust of institutions, cynicism about our leaders, and skepticism about our ability to solve social problems.

Second, the problem of foreign disinformation is almost surely going to get worse, and will pose serious national security threats against which our military prowess will be largely ineffective.

Third, while it may be difficult, there are indeed steps we can take to counter these threats.

Returning to my first point, with three out of four Americans getting some or all of their news from social media platforms, disinformation could specifically affect our military in concerning ways.

At the most basic level, the resulting cynicism, or lack of trust in our military, as was revealed in the recent Reagan Institute survey, might well erode the national consensus underpinning congressional appropriations for weapons systems or veterans affairs, and more directly, recruiting for our all-volunteer military forces.

Border threats to our military arise from our foreign adversaries' use of disinformation as a tool of their statecraft. For example, China's concerted online campaign to deflect investigations into the cause of the COVID–19 outbreak, to paint themselves as successful in curtailing the virus when Western democracies have been floundering, and to deny their militarization of the South China Sea, all complicate, if not undermine, our foreign relations and heighten the chance for conflict.

The second point is that foreign cyber-propelled disinformation is likely to get much worse, to the extent that we would have difficulty in fending off weaponized disinformation coming from a sophisticated foe.

Indeed, the recent final report of the National Security Commission on Artificial Intelligence cited a, quote, "gathering storm of foreign influence and interference," and asserted that our foreign foes will use artificial intelligence systems to enhance their disinformation campaigns, including by creating undetectable, deep-fake videos and audio recordings.

The resulting skepticism, treating official and counterfeit news sources equally, would yield a chaotic and unreliable reality in which truth and genuine information are elusive.

The seemingly inexorable trajectory of ever-worsening foreign cyber attacks from Russia, China, Iran, and North Korea, shows us what online disinformation will look like from those adversaries.

The same factors that shield them in cyber malevolence, the uncertainty of provable attribution, and the absence of directly caused actual injury or physical damage, will also work even more effectively to insulate them as they inevitably step up their disinformation campaigns.

What if next time Russia or Iran seizes on a natural disaster, say, a hurricane or flood, and weaponized the crisis with false information online about the hurricane's path or expected river crestings, or even wrong instructions about escape routes?

We don't need to wait until such a crisis or a disaster. The very fact that there are many sources contributing to disinformation means that we have multiple ways to stem it.

I would be happy to respond to your questions about specific solutions, but I will concede that responding to the challenges of disinformation will not be easy, since it will require making difficult and controversial decisions about the responsibility of the private sector for our national well-being, and about restrictions on speech.

But it isn't impossible, and Congress, in concert with the private sector, should lead the way. Our national well-being depends on

nothing less. Thank you for the opportunity to present my views to the subcommittee.

[The prepared statement of Mr. Gerstell can be found in the Appendix on page 34.]

Mr. LANGEVIN. Thank you very much, Mr. Gerstell. Thank you for your testimony, and we appreciate having you here.

We will now receive testimony from Ms. Nina Jankowicz. Ms. Jankowicz is a disinformation fellow at the Center—excuse me for a second—yeah, it is—Ms. Jankowicz is a disinformation fellow at the Wilson Center, and is the author of "How to Lose the Information War: Russia, Fake News, and the Future of Conflict."

Ms. Jankowicz, thank you for being here. You are now recognized to summarize your testimony for 5 minutes.

STATEMENT OF NINA JANKOWICZ, DISINFORMATION FELLOW, WILSON CENTER

Ms. JANKOWICZ. Thank you Chairman Langevin, Ranking Member Stefanik, distinguished members of the subcommittee, it is an honor to testify before you today.

I am the daughter of a veteran. My father, an aerial reconnaissance officer in Vietnam, died in 2010 from complications from multiple myeloma which he contracted as a result of his exposure to Agent Orange during his service. I know he would be thrilled to see me testifying before you today in the service of truth.

I spent my career on the front lines of the information war. We all now seem to recognize that the threat exists, but as I told your colleagues on the Appropriations Committee in 2019, the United States has been a tardy, timid, or tertiary player, stymied by domestic politicization.

Unfortunately, nearly 2 years later, we are in the same place. So it bears repeating. Disinformation is not a partisan issue. As we witnessed throughout the COVID–19 pandemic, and on January 6th, it affects public health, safety, and our democratic process. It is crucial that Congress understand this. Otherwise, we remain vulnerable.

How did we get here? In part, we haven't understood the scope of the problem. The U.S. thinks of disinformation as a string of one-off occurrences that warrant attention only in the moment. We haven't created a comprehensive, long-term defense plan, and there is too little recognition of the need to shore up domestic vulnerabilities.

Russia, China, and other authoritarian states know how to exploit this. They take advantage of American inaction, engaging in perpetual information competition, which has three characteristics.

First, adversaries understand information competition is the new normal, and they are constantly probing for societal fissures to exploit. We have seen this with conspiracy theories about the origins of COVID–19 and the efficacies of Western vaccines. And Russia, of course, has an ongoing campaign to exacerbate racial tensions in the U.S.

Second, they use all channels available—government and non-government, online and offline. China, for example, uses a wide range of state bodies, not just traditional national security bodies,

to influence Western opinions about protests in Hong Kong, and more recently, to paint a positive picture of life in Xinjiang.

Third and finally, they use perpetual information competition to target alliances and international organizations. For instance, Russia waged a campaign to prevent Ukraine from signing an association agreement with the European Union in 2016.

In short, hostile state information operations increase domestic tension, and decrease American resilience. To meet the challenge of perpetual information competition, the Department of Defense should organize itself around a posture of enduring information vigilance, a concept I developed with my colleague in the U.K. Cabinet Office, Henry Collis.

It is composed of the three Cs. The first is capability. We should remember the old military adage: Don't operate the equipment, equip the operator. The DOD workforce should be able to proactively monitor and identify informational vulnerabilities.

Section 589E of the 2021 NDAA [National Defense Authorization Act], which trains Active Duty personnel, their families, and civilian DOD employees in detecting information operations, is an excellent starting point. Such a training program could also be rolled out to all civil servants across the Federal Government.

The second C is interagency coordination. DOD and the wider USG [United States Government] must break out of our siloed national security thinking. To remedy this, the National Security Commission on AI recommends the creation of a joint interagency task force to coordinate intelligence and information-sharing around IO [information operations].

I agree that the Federal Government requires a central mode for monitoring disinformation and coordinating policy, ideally in the White House, but my research across Europe suggests we also need the involvement of nontraditional security departments.

In the long term, the key to combating disinformation lies with departments focusing on education, arts, and health, at Federal and local levels, as well as building a thriving, pluralistic media environment and teaching civics.

The third C is international cooperation. This includes better sharing of information to identify threats and formulation of effective responses with allies.

Toward this goal, the NSCAI [National Security Commission on Artificial Intelligence] suggests an international task force, led by the Global Engagement Center [GEC] at the State Department. However, the GEC's agreement is too large, its budget too small, and its reputation within the interagency and international communities too uncertain to add such a task to its portfolio.

It currently produces open-source intelligence analysis, in addition to its coordination, policymaking, and analytic roles. And I recommend that intelligence-gathering rest with analytics, not policy bodies.

The GEC's limited resources are better allocated in coordinating with embassies and other agencies in establishing and implementing policy and program priorities.

Finally, while the idea of a task force for international coordination is a noble one, the U.S. must recognize that we are arriving late to this party. We should augment efforts that are already un-

derway by close allies such as the U.K.'s international partnership for countering state-sponsored disinformation, and the G7 Rapid Response Mechanism.

Enduring information vigilance cannot be built overnight. It requires a long-term commitment that will likely outlast the current political class, but the result will be a more resilient society.

The United States must act not only as the staunchest defender and guarantor of democratic values among our allies abroad, but actively lead by example, underlining that disinformation knows no political party, and that America is committed to reversing the normalization of disinformation in our own political discourse.

Once again, thank you for this opportunity, and I look forward to your questions.

[The prepared statement of Ms. Jankowicz can be found in the Appendix on page 47.]

Mr. LANGEVIN. Very good. Thank you, Ms. Jankowicz.

We will now receive testimony from Dr. Herb Lin. Dr. Lin studies cyber policy, information warfare and influence operations, and is a senior research scholar at Stanford University. He is the author of "Bytes, Bombs, and Spies."

Dr. Lin, you are now recognized to summarize your testimony for 5 minutes.

STATEMENT OF HERBERT LIN, SENIOR RESEARCH SCHOLAR, CENTER FOR INTERNATIONAL SECURITY AND COOPERATION, STANFORD UNIVERSITY

Dr. LIN. Thank you, Chairman Langevin, Ranking Minority Member Stefanik, and distinguished members. Thank you for inviting me to testify today. I am speaking for myself today, and not on behalf of any institution.

The general thrust of my remarks is that Department of Defense is poorly structured and equipped to cope with the information warfare threat facing the U.S. as a whole. However, the DOD can make a meaningful contribution in addressing part of the problem.

We usually believe in a clear distinction between peace and war. Today, we are not in a shooting war with Russia or China, but we are not at peace either. Our adversaries prosecute the state of "not peace" in many ways, including cyber-enabled information warfare.

Such warfare presents several new challenges. First, the Constitution is the foundation of U.S. Government. Deeply embedded into the Constitution is the concept of a marketplace of ideas. Here ideas publicly compete with each other, and truth emerges from public debate of ideas.

But this concept emerged at a time when information was hard to obtain. Today the internet and social media have brought a deluge of information so great that no one can possibly access or process all of the information needed to evaluate any given idea.

The second challenge is that the information marketplace presumes that people process information rationally, thoughtfully, and deliberately. However, psychological science has demonstrated that people often do not do so. Instead, they often make fast, intuitive judgements based on how they feel from their gut, even though everyone is, in fact, capable of thoughtful deliberation.

Such judgements—fast intuitive judgements from the gut—are usually adequate for the kinds of personal decisions found in everyday life, but they are inadequate when the consequences for error are high.

Moreover, many of our tech companies have learned that supplying content that plays to our worst habits of nonrational thought is the way to increase user engagement which, in turn, increases their profitability.

Third, the boundaries between foreign and domestic sources of information chaos are blurring. Russians and Americans may not be working side by side to sow disorder, mistrust, and polarization in the United States, but the scope, nature, and effect of their activities, even if separately conducted, are largely indistinguishable.

That means, any effective effort against Russian activities will inevitably have collateral effects against American activities that are similarly oriented.

In sum, the information warfare threat to the United States is different than from past threats, and has the potential to destroy reason and reality as the basis for societal discourse, replacing them with rage and fantasy.

Perpetual civil war, political extremism waged through the information sphere and egged on by our adversaries is every bit as much of an existential threat for American civilization and democracy as any military threat imaginable.

Why can't DOD defend effectively against the information warfare threat? Fundamentally, it is because the information warfare threat requires a whole-of-society response, and DOD cannot, and is not in a position to, orchestrate such a response.

More specifically, DOD policy directives prohibit information operations directed at U.S. audiences, regardless of the intent underlying them, and that includes activities intended to protect U.S. audiences against foreign information warfare operations.

But there are also cultural constraints. DOD culture is oriented towards defense against physical threats—planes, missiles, and the like. But DOD was never designed to defend against nonphysical threats. Joint doctrine does not even acknowledge the possibility that the U.S. Armed Forces could be the target of adversary psychological operations.

Nevertheless, despite existing policy and culture, DOD is well-positioned to assess the information warfare threat for at least one segment of the U.S. Government, namely the Armed Forces and their families.

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 the vast majority receive no education, no instruction, on what these words mean.

The fiscal year 2021 Defense Authorization Act called attention to the need to protect U.S. military personnel and their families from foreign malign influence and disinformation campaigns, that was the previously mentioned section 589E, and both Secretary Austin and the Congress have expressed concerns about extremism in the U.S. military, which is facilitated by exposure to foreign disinformation campaigns.

These points suggest the need for DOD to provide substantial in-house training for military personnel on the meaning of their oaths and on civics education as a prerequisite foundation for such training.

That concludes the oral portion of my testimony. Thank you for the opportunity. I am happy to answer any questions.

[The prepared statement of Dr. Lin can be found in the Appendix on page 60.]

Mr. LANGEVIN. Thank you very much, Dr. Lin. Appreciate you being here as well.

We will now receive testimony from Dr. Joe Kirschbaum.

Dr. Kirschbaum, welcome back, and thank you and your team for all the recent support. Dr. Kirschbaum is the Director of the Government Accountability Office Defense Capabilities and Management Team. Dr. Kirschbaum, you are now recognized to summarize your testimony for 5 minutes.

STATEMENT OF JOSEPH W. KIRSCHBAUM, DIRECTOR, DEFENSE CAPABILITIES AND MANAGEMENT TEAM, GOVERNMENT ACCOUNTABILITY OFFICE

Dr. KIRSCHBAUM. Chairman Langevin, Ranking Member Stefanik, and members of the subcommittee, I am pleased to be here today to discuss the vital role of the Department of Defense's operations in the information environment.

Throughout history, militaries and states have sought advantage through actions intended to affect the perception and behavior of adversaries. As we have noted today, our adversaries, particularly China and Russia, are taking advantage of emerging information technology to offset the United States conventional warfighting advantages.

Although we focused on the Department of Defense, to reiterate, as an element of U.S. national power, information operations, as a whole, are necessarily part of a whole-of-government and whole-of-society effort.

My testimony today describes the Department of Defense's information operations concepts, and DOD's actions to implement the 2016 strategy and address information operations challenges. This statement is based on reports we issued in late 2019 and our assessment of defense information-related documents.

The terms for information operations—doctrinal terms—are many and varied. DOD has defined some, but inconsistency and potential confusion remains. Among the things the Department is actually working on right now is a more consistent set of information operations-related terms.

To achieve greater effects in the information environment, combatant commanders can plan and execute operations that combine multiple information-related capabilities.

Such capabilities include military information support operations, what was traditionally known as psychological warfare; military deception; cyberspace operations; electromagnetic warfare; operation security; and special technical operations.

There are, however, many other related capabilities, such as public affairs, civil-military operations, and intelligence capabilities.

A good example of an information operation is the effort by the Allies in 1944 to convince the Germans that the attack on occupied Western Europe would come at a place other than the actual target of Normandy.

Operation Fortitude involved a number of what we would now call information-related capabilities. These included creation of fictitious military units, with all the requisite paperwork, associated radio transmissions and traffic, and assigning a real U.S. Army General—in this case, George S. Patton—to command those units.

It also involved the creation of mock aircraft and landing craft located in southeast England, and many other intelligence and military deception techniques.

While this is on a grand scale, defense planners today can do the same kinds of things to integrate more than one information-related capability to achieve desired end states.

DOD's 2016 Strategy for Operations in the Information Environment was intended to significantly enhance their ability to conduct information operations today. However, the Department did not fully implement that strategy, leaving approximately 80 percent of the enumerated tasks incomplete.

Among the largest omissions was the absence of an implementation plan, or an investment framework. The Department instead shifted focus to develop a joint concept of operations and a capabilities-based assessment. Both worthy efforts. It then started to develop a new strategy, which remains in development.

We also found gaps in DOD's leadership, oversight, and management. The Department assigned most responsibilities to the Under Secretary of Defense for Policy. However, delegating many of those responsibilities down to a lower level and failing to formalize authorities exacerbated the dispersal of leadership and focus.

As you pointed out, Mr. Chairman, congressional direction has prompted movement in the Department. In fact, most movement. Examples include the new information operations cross-functional team, which may mitigate some of the problems we identify, and designation of the Under Secretary of Defense for Policy as the principal information operations adviser, reporting directly to the Secretary of Defense.

Ultimately, however, the leadership the principal adviser exercises, and the support the Department gives them in implementing Department-wide strategy and vision, will be critical.

DOD has integrated information-related capabilities in some military operations but has not addressed key planning, coordination, and operational challenges. This is important for ensuring that DOD integrates the information dimension into routine operational planning.

DOD resisted our recommendation to conduct a comprehensive posture review in order to assess challenges. However, once again, Congress subsequently required the Secretary of Defense to conduct such a posture review.

DOD told us they have taken initial steps to conduct this review, but did not provide an estimated completion date.

In summary, there are opportunities for improved DOD leadership, recognition of information as a joint function, and better pre-

paring the military to conduct information operations and counter our adversaries.

I look forward to continuing to work with this committee, and the Department, to help it address these challenges and make the most of these opportunities.

Chairman Langevin, Ranking Member Stefanik, and members of the subcommittee, this completes my prepared statement, and I am happy to respond to any questions.

[The prepared statement of Dr. Kirschbaum can be found in the Appendix on page 80.]

Mr. LANGEVIN. Very good. Thank you, Dr. Kirschbaum, and I want to thank all of our witnesses for your testimony today. You do a great service to the subcommittee and to the committee at whole, writ large, by appearing today and giving us your perspective.

Dr. Kirschbaum, let me start with you. So Congress has consistently encouraged the Pentagon to focus on these issues, including requiring the DOD to create a principal information operations adviser. Has the Pentagon sufficiently elevated dedicated information operations leadership?

Dr. KIRSCHBAUM. Mr. Chairman, I would say yes and no. So, in brief, what has happened with the diffusion of leadership, for example, most of the responsibilities for information operations was delegated down to the level of the Deputy Assistant Secretary for Special Operations and Combating Terrorism.

As that title indicates, that is a lot to work on, and so, incorporating information operations into that very small staff has generated issues. While very capable, they are not at the right level, in a lot of cases, to achieve some of the results because of that lack of leadership.

Now, the Department has gone back and identified the Under Secretary of Defense for Policy as the principal information operations adviser in the hopes that keeping it at that level will elevate importance.

And the comparison, of course, is made to the situation with the principal cyber adviser. There are some differences that we are a little concerned about, seeing how the Department carries through with that.

For example, the principal cyber adviser had a deputy who could leverage a deputy assistant secretary who was focused solely on cyber operations. The Under Secretary of Defense for Policy, as you appreciate, is doing just a few things. So, focusing on information operations will be important to see what level of resources, what level of attention it gets, assuming it is at that right level, assuming they are able to assign a deputy with the right focus, and, then, follow through with the right structural, procedural impetus in order to make sure momentum continues.

Mr. LANGEVIN. Thank you. Thank you for that answer. Mr. Gerstell, can you further explore why foreign-enabled malign influence and disinformation are a national security threat? And how will emerging technologies, like artificial intelligence, increase this threat?

Mr. GERSTELL. Thank you, Mr. Chairman. So, I think we have rich evidence of the fact that foreign-inspired disinformation is a

real national security threat. The 2016 elections were certainly a good example of that with, as you know, the Senate Intelligence Committee issued a five-volume bipartisan report finding that Russia actively intervened in our elections in an effort to influence them in 2016.

It is hard to say for sure exactly what the result would be, but anybody would think that tampering with our democratic process must—must—by definition, be a national security issue.

We have certainly seen how foreign disinformation from China and Russia, which just this week, once again, was touting the virtues of their Sputnik vaccine, and degrading the virtues and qualities of the American Pfizer and other COVID vaccines, clearly disinformation that is going to hurt our public health, the ability of Americans to get vaccinated. Again, another effect on national security.

If we want a very specific example, just quickly, back in last September, when there were terrible wildfires in Oregon in the Northwest, Russia jumped on a couple of misleading and false statements that were set forth in some QAnon accounts and really weaponized them. They, in a concerted, coherent way, amplified them and turned them into a detailed, rich story of falsehoods about who started the wildfires, claiming that Antifa protesters were doing it.

It reached a point, because of what Russia was doing, that civilians actually set up roadblocks in Oregon, in effort to stop these perceived but erroneous protesters who, of course, weren't there. It actually hurt people who were trying to flee the fire, so much so, that the Douglas County Sheriff and the FBI [Federal Bureau of Investigation] pleaded with the public to stop circulating these falsehoods.

So we have seen how foreigners can take an existing division and create national security problems here on our soil. It stands to reason, following your other question, Mr. Chairman, that using technology—artificial intelligence—to micro-target viewers and listeners will only exacerbate the problem. So that is why I said, I believe the problem has the potential for getting worse before it gets better.

Mr. LANGEVIN. And from your vantage point, what can the United States do to protect itself from both a technological and policy standpoint?

Mr. GERSTELL. I think there are a wide range of tools. As I said in my earlier comment, and I know the other panelists agree with me here, disinformation has many causes. So the fact that it has many causes means that we also have many ways of treating it, to use a—sort of a medical analogy. This is a chronic condition, a complex chronic condition. So it is not a disease that will be cured by one miracle drug.

So, I think we have a rich opportunity to use a range of legal tools at our disposal, perhaps by tightening up section 230 of the Communications Decency Act, perhaps by either causing the industry to self-regulate, or to regulate the ability of social media platforms to limit the virality of falsehoods to check them before they get spread too widely.

We can take steps in our society to increase, as others have said, digital literacy, civic education, so that people will have a better understanding and will be better able to assess falsehoods.

I think the most important thing—and I am echoing what Ms. Jankowicz just said, and you, Mr. Chairman, also—is, we need an integrated approach to this. Russia and China use an integrated approach, a whole-of-government and their private sector, to create these disinformation campaigns.

There is an asymmetry. We don't. We need to do that, and that will be the key to success in this area.

Mr. LANGEVIN. Very insightful, well said, and I couldn't agree more. Thank you.

My time is expired. I am going to now turn to Ranking Member Stefanik for her questions.

Ms. STEFANIK. Thank you.

My question is for Dr. Lin. In the past, the special operations community and service members in the field of PSYOPs [psychological operations] and civil affairs had the most experience with information operations. It is going to be very important that the Department scale these skills to a wider force. How do we do that, and specifically how do we equip our cyber forces with the skills to conduct effective information operations?

Mr. MOORE. Mr. Lin, you are on mute still.

Dr. LIN. All right. Thank you. Ranking Minority Member Stefanik, thank you for asking the question. I hate technology.

How do we get the cyber forces to be better able to address the influence operations side of the house? That is a question—I addressed that in the paper that I submitted for the record, on dysfunction in the DOD about doctrine and so on.

The short answer is that I believe that there needs to be a joint—something that is joint and standing, some effort, some entity, that pulls together the cyber people together and the PSYOPs people together, as equals.

Cyber Command has the expertise in the information delivery side of the house. The PSYOPs people, the MISO people, have the responsibility of understanding content, and those two have to be put together.

For me, trying to grow psychological expertise out of what are fundamentally a bunch of technical hackers, as good as they are, that is not their skill set. Their skill set is flipping bits, and so on.

I speak as a former bit-flipper myself, and getting the psychological insights from others who are much more expert in that, I think, is the way to go.

So there has to be a standing team, and the standing part is really important, because it recognizes the fact that this is an ongoing problem, not one of a specific campaign here or there.

Ms. STEFANIK. Yield back.

Dr. LIN. I hope that answers your question.

Ms. STEFANIK. It did. Thank you. Yield back.

Mr. LANGEVIN. Thank you very much, Ranking Member Stefanik.

Mr. Keating is now recognized for 5 minutes. Is Mr. Keating still with us? If so, you might be on mute.

Okay. If Mr. Keating is not there, in the tradition of going Democrat, Republican, I will just go down the list to Mr. Morelle.

Mr. MORELLE. Thank you very much, Mr. Chairman. This is really a fascinating subject. And I am new to the committee and the subcommittee, so I am not entirely familiar with DOD's actions. But having listened now, and I hear that there is calls for more coordination, more information-sharing, greater intentionality of our focus, but I am still struggling, just as a layperson, to suggest what you have offered as recommendations that would actually stop the disinformation from seeping in. Given that we have an open and democratic society, given that we have social media, how do we actually stop this, other than—well, I am just sort of curious.

What are the tactics and the strategies we use to prevent this from really undermining society here in the United States and really creating more divisiveness?

Ms. JANKOWICZ. I am happy to jump in there. Thank you, Congressman, for that question. You are absolutely right. There is not very much that we can do to instantaneously correct this problem. Right now, and for the past 4 or 5 years, we have been playing what I call "whack a troll," where we want to just focus on offensive content, harmful content, but really we need a much more systematic and, in fact, endemic solution.

And our adversaries—Russia, China, Iran—have been playing the long game, they are playing a generational game. They are not necessarily interested in getting it right every time, but they know that if they can chip away at the surface, eventually they are going to get to the core of the polarization that they are seeking for, and keep us distracted so that they can do whatever it is that they are looking to do in their near abroads, domestically, with regards to human rights, et cetera, as well as achieve political goals.

So that is why, in addition to focusing a little bit on content moderation, which is the topic du jour, right, in addition to making sure that our government bodies are putting out authoritative information, that it is trusted by the public, that is why we really need to start investing in what I call citizens-based responses.

So all of the countries that I have studied in Central and Eastern Europe that have been dealing with Russian disinformation for much longer than we even recognized it existed, have all, of course, looked at the kinetic side of things. They have good cyber defenses, but they also invest in their people.

And I know that is out of remit of this subcommittee, but it just speaks to what Mr. Gerstell, Mr. Lin, and Dr. Kirschbaum have all touched on, that we need a whole-of-society response, and we really need to get out of this siloed national security thinking, invest in libraries, invest in public media, so that people have trustworthy sources of information to go to, and invest in awareness and civics, so that folks understand their role in the democratic process, because ultimately, that is what disinformation is trying to undermine—people's participation.

Mr. MORELLE. Look, yeah, I appreciate that, and I certainly don't want to be argumentative. I read recently Anne Applebaum's, the Twilight of Democracy, which is a frightening volume, similar kinds of lines of communications. But what troubles me is, I can certainly envision foreign adversaries starting to spread, through social media and otherwise, arguments that a Presidential election, for instance, was stolen from the American public, and despite a

lot of investigation, no evidence ever emerges that such a thing happened.

And yet, you can imagine potentially a third of the American public believing that no matter, and that really gets at the foundations of American democracy. I think I would like to believe that that wasn't possible, but frankly, I feel like I just lived through this nightmare.

And, so, I appreciate what you are saying, and I don't disagree with you, I am just really, really concerned that there may not be an answer. And I don't know that it is the Department of Defense's job. I don't even know how they would begin to do this, but having listened to all three of you, I just struggle with, like, okay, so what, if anything, can we do here?

And I apologize, I am using up a lot of time, but if the other two witnesses want to respond, I would love to hear your thoughts as well.

Dr. LIN. I would say, starting with education of the Armed Forces is a big step forward. Getting the people whose job it is to protect us and defend the Constitution, teaching them what it means to do that, getting them some real education, that is a meaningful step forward——

Mr. MORELLE. I am not sure—I mean, I don't mean to disagree with you. I think that is a great suggestion. We couldn't even get Members of the House of Representatives to defend the Constitution this past November against a suggestion that an election was stolen with no evidence that that is the case. I am not sure—if we can't get the Congress to do it, I don't know how we would get members of the United States military to do it. But again, I don't mean to be argumentative. I am just frustrated, and I think probably all of you are with where we find ourselves.

Mr. GERSTELL. Congressman Morelle, if I may add to that——

Mr. MORELLE. Sure.

Mr. GERSTELL [continuing]. I certainly share your frustration. I suspect probably everyone on both sides of, metaphorically, of the witness table, so to speak, feels that. But the Supreme Court has been very clear that Americans have a First Amendment right to receive foreign disinformation, no matter how outrageous it is.

Some philosophers talk about the paradox of tolerance, which is that a society that is very tolerant and open to lots of views, also potentially has the seeds of its own destruction, of course, because someone could criticize the very society. So you are right.

I think the best analogy, just very quickly, is the cybersecurity one, which is, I think cybersecurity experts will tell you that at the end of the day, we are probably never going to be able to completely eliminate cybersecurity attacks from a sophisticated foreign adversary.

Instead—and we should certainly work on that, but instead, what we need to do is limit their effectiveness and their scope. And I think it is the same thing with disinformation. We are not going to stop it where it starts, overseas, but we can limit its effectiveness on our soil.

Mr. MORELLE. I have well exceeded my time. Mr. Chairman. Thank you for your indulgence, as I am glad you gave the gentleman an opportunity to answer, and I yield back.

Mr. LANGEVIN. Sure. Thank you, Mr. Morelle.

Now I would like to recognize Mr. Moore for 5 minutes.

Mr. MOORE. Thank you, Chairman and Ranking Member. It is clear, and I think I want to just—a sentiment that was given a few minutes ago, we can't even just keep this with respect to the Department of Defense. Cyberspace, this threat, is in every aspect of our lives, from banking, entertainment—I mean, across the board. So just to emphasize the importance of this, and when we do think about our defense-related work, our legacy platforms, our legacy weapons platforms, they still serve a valuable deterrent.

But electronic warfare and cyber operations are central to the future fight. I will keep my questions geared towards that, and making sure we can be thinking about the future. And, so, I will start with a question to Mr. Gerstell.

We have heard in this committee that the artificial intelligence capabilities of our adversaries are rapidly progressing to the point where it can only be combative with our own AI technologies. Can you just give us some perspective? Is the United States winning this AI arms race? If not, what steps need to be taken to increase our competitiveness?

Mr. GERSTELL. Sure. Thank you very much, Congressman. I think the best answer I could give would be to point to something that has already been alluded to, which is the final report of the National Security Commission on Artificial Intelligence, which has a rich series of recommendations for our Nation to invest in, ranging from everything from educating our workforce, to stepping up government investment, working with the private sector to increase AI, and perhaps—and also, including a series of laws, ultimately, and recommendations on limiting the use of AI for beneficial purposes and limiting its misuse.

So we are in an arms race, so to speak, principally with China, on the area of artificial intelligence. They are busy amassing data, including data on Americans, that could be very significant when coupled with artificial intelligence and machine learning, and used against us in nefarious ways.

So, we have our work cut out for us. I think there is a large series of recommendations that I would endorse of the Commission, and that would be a very, very important step for us to go down that road.

Mr. MOORE. Excellent. Thank you.

On that same topic, Dr. Lin, Chinese and Russian militaries are structured to integrate information-related capabilities, and are absent of any genuine oversight, I will say. How can the DOD refine their current management structure to improve synchronization of information capabilities, while maintaining the merits of civilian control of the military, where we, as a Nation, will always, you know, have proper oversight to the extent possible, and knowing that we don't always get to fight against nations that don't value that as much as we do. But is there improvements that we can make to level the playing field?

Dr. LIN. Well, one of the things that I—certainly one of the things that I have thought about is, for example, the distinction that this committee is very well aware of, the distinction between title 10 and title 50 authorities.

A large part of this game is done in the intelligence world, sort of in the covert-action world. Systems operations are often covert, and it is an interesting question as to how—whether—how and to what extent coordination between title 10 and title 50 authorities, I have heard people say that you should—we need a title 60, you know, as a combination of the two, to better coordinate.

It is very hard, as long as we are very concerned about authorities, to achieve the kind of coordination that you are talking about. Neither the Chinese, nor the Russians, are really worrying very much about who has the authority to do [inaudible]. It is hard to imagine [inaudible] whether something happens because one branch does it or another branch does it, but we care a lot about that.

Mr. MOORE. Okay. Excellent. Thank you. For a final question, Ms. Jankowicz, first off, I was touched by your comments on your dad, and I am sorry to hear that, but I am sure he is proud of you.

Anything you wanted to highlight in this platform, just on some of the things that we are doing right, and as meetings that I have had recently with some of the cyber companies in my neck of the woods out in Utah, like small business and smaller operations are being more nimble, is there an opportunity to leverage those types of more—I guess I will just reuse the term nimble—organizations to help fight this battle going forward?

Ms. JANKOWICZ. Yeah, absolutely. Thank you, Congressman, and thanks for your comments about my dad.

I mean, I think, finally, the fact that we are recognizing this problem, that these hearings are happening more frequently is a good thing. And the fact that this is a bipartisan showing here in this committee warms my heart frankly, and the leadership that you all show is really important in setting an example for your constituents, for the media, for everyone. So kudos on that.

I do really think we need a central node in the Federal Government, not only to work on the intelligence issues, which we heard from ODNI [Office of the Director of National Intelligence] is going to be happening soon within ODNI, but we need somebody to be setting policy, and I think that is where DOD and the GEC, and other bodies in DHS [Department of Homeland Security], like CISA [Cybersecurity and Infrastructure Security Agency], for instance, are kind of operating all in their own spheres. So I would like to see a lot more coordination.

And on a local level, I think you are absolutely right. We need to really create and invest in more robust public-private partnership in this area, not just with the Big Tech firms, but with local businesses and with civil society organizations.

You know, the most successful programs to counter disinformation that I have seen around the world have been ones that invest in those local connections, with local media, local civil society groups, local libraries, even local influencers and performers who can go there and deliver an authoritative message to folks that they are neighbors with, without, you know, the baggage of it coming from the Federal Government.

So I think we need to think a lot more creatively, a lot more out of the box, and business, local business, is a great place to start with that.

Mr. MOORE. Thanks for the thoughtful comments, and I yield back. Thanks for that.

Mr. LANGEVIN. Thank you.

Mr. Larsen is now recognized for 5 minutes.

Mr. LARSEN. Yeah, thanks, Mr. Chair. I appreciate it. Greetings from the Pacific Northwest, where you will not be surprised to know it is raining today. So thanks for the chance to say hello.

My first question is for Dr. Kirschbaum. I usually embrace everything the GAO [Government Accountability Office] says. I want to preface my comments. I do want you to explain a little bit more on the recommendation. We are moving to criticism about the delegation that the U.S.—or under the theory defense policy makes on MISO operations, in particular, to special operations forces. I think your characterization that special operations forces focused quote, "only on special operations and counterterrorism" might have been accurate 10 years ago, is inaccurate today. In fact, there is a bit of a debate going on about the role special operations needs to play in great power competition, which, in part, includes information operations, but specific to special operations.

So can you talk a little bit about how you approach that particular question, and then relate that to a broader comment about how the Pentagon is organized? And could you grade that for us, for information operations?

Dr. KIRSCHBAUM. Mr. Larsen, thank you so much for your question. So, first, I want to make sure that my comments are not misunderstood. You are correct that the idea of Military Information Support Operations, PSYOP. That is exactly where that user belongs. That is where that specialty is. It is in special operations, and then the combination for intelligence. That is true.

The comment that I made really has to do with the decision by the Department to move information operations writ large into that space where you have very few people. And I have had the great opportunity to work with most of those people, and they get it, they understand what needs to be done. They have written a lot of the things in the direction that kind of point the way to where the Department is going. However, I think they are a little stymied in being able to get traction in the rest of the Department to look for.

So, for example, when we talk about what you have to do to kind of inculcate info operations and understanding throughout the Department. It kind of goes to what Dr. Lin was talking about, you need a broader, joint understanding. And, so, you take advantage of those individual specialties, like MISO, you take advantage of cyber, you take advantage of all these other things, but you do it in a way that everyone understands how to integrate that, which is why I said it needs to be integrated, operationally, into the planning cells for the J–2s, the J–3s, and the J–5s at all the COCOMs [combatant commands].

In terms of Department leadership, it really doesn't matter who has got the ball, as long as there is Department-wide emphasis and momentum. And that is what we have seen lacking. And depending on a very small number of people to carry the ball to implement the strategy, to carry out the capabilities base assessments, to do all the things we have asked them to do over and over again, it hasn't worked. They haven't got the traction throughout the De-

partment. They have not gotten the support they need. That is where the potential for identifying the principal information operations adviser, keeping it at the level it is, and then rely on those existing staff, and giving them the support is hopefully the way to make that stick.

Mr. LARSEN. Yeah, maybe when either this subcommittee or the full committee has an opportunity to talk to Under Secretary of Defense [for] Policy Kahl about his view on this now that he has been approved by the Senate, or by the Senate, we can have a chance to talk to him.

I noted that the clock didn't start exactly on time, but it was adjusted, so I will assume I do have a minute 40 left, and go to Ms. Jankowicz.

Because the Pentagon is the Pentagon, and because it has to operate outside, not inside, the country, how should we look at fitting the Pentagon IO function in this largely—in a larger coordinated fashion with other government operations?

Ms. JANKOWICZ. Thank you, Congressman. I think the important thing here, again, is the central node. So taking under account the defense intelligence gathering that is going on, sharing that in the interagency, making sure that priorities out in the field in our areas of conflict are lined up with what the Department of State is doing in their programming. And then again, I think the Department of Defense has an opportunity to really be the laboratory for educating the Federal workforce about information operations. They are certainly a targeting bio. Their families are. And there have been multiple studies about catfishing and other things against the Armed Forces.

So, educate them and then roll that out more broadly to the rest of the Federal workforce. And I think it is the biggest opportunity that the Department of Defense has with this challenge.

Mr. LARSEN. Yeah, good, thanks. Thank you very much. And thank you, Chair Langevin. I appreciate it very much. I will yield back.

Mr. LANGEVIN. Thank you, Mr. Larsen.

Let's see, Mr. Fallon, is recognized for 5 minutes.

Mr. FALLON. Thank you, Mr. Chairman, I appreciate it.

Mr. LANGEVIN. Thank you, Mr. Fallon.

Mr. FALLON. Can you hear me? Sorry.

Mr. LANGEVIN. Yeah go, ahead.

Mr. FALLON. Oh, wonderful. Thank you. I wonder if the panel can answer some questions. One of which is, amongst rule of law Jeffersonian democracies in the world, what countries are the gold standard? [Inaudible] emulating vis-a-vis cyber disinformation?

Ms. JANKOWICZ. Well, I can jump in there, Congressman. In my research I look at a number of countries in Central and Eastern Europe, again, that have been dealing with this for decades now. Estonia is one I always like to bring up. Of course, it is quite a small country, only 1.3 million people. But in 2007, they were hit with a cyber attack as well as what I call beta disinformation, pre-social media, at the hands of the Russians that caused a riot, that caused one person to die. And the cyber attack, of course, took down their banking as is well known, and many of their other E-governance operations in Estonia.

And that was a real wake-up call, along with kind of a reinvigoration during the annexation of Crimea in 2014. And as a result, the Estonian Government is really invested in cyber operations, they have invested in Russian language media, to reach out to that disenfranchised population. And they have invested in really building trust between the Estonian Government and the ethnic Russian population there.

And I think that is a great model for a whole-of-society, a whole-of-government solution. And if fluffy little Estonia can do it, I think that the United States of America should be able to do something similar as well.

Dr. LIN. I was just going to say that Finland also is another example of whole-[inaudible]-country, whole-[inaudible]-society approach to disinformation. They have been dealing with it for a lot longer than most of the other countries in the world. And they emphasize this throughout society, and it is very much a part of their educational regime.

Mr. FALLON. Is it fair to say that Russia is the most adroit at this, or is China catching up, or are they on par?

Dr. LIN. Different people have different judgements about that. I think the Russians are most pernicious because they—it is easier to tear down stuff than it is to build something up. And the Russians are extraordinarily good at tearing stuff down. And the Chinese are getting there, but for my money, it is the Russian threat that I am most concerned about right now.

Mr. FALLON. I think the Russians had 600 years of practice in that regard. What are we doing as far as offensively to combat this? Because we don't need to—we just need to get out information in a lot of ways when we are talking about totalitarian regimes and giving it to their people. Are we taking specific—because you know, the old adage is the best offense—or the best defense is a good offense. Are you all aware of efforts that we have that we are making, and do we need to focus more on that as well?

Dr. LIN. I just had a little bit in my written testimony. I think that the biggest policy question that we have to—that we have to address as a country, is how and to what extent, if at all, we should be adopting the techniques of the Russians in prosecuting information for their offense. I am going to point out that our offensive information worker efforts don't help defend the United States, and defense information warfare can only influence other populations.

Do we want to adopt the tactics of the Russians in this? I am very uncomfortable about that as an American citizen. On the other hand, it is pretty clear that speaking the truth, just the truth, doesn't work very well. And Americans believe that speaking truth, that the truth will eventually win. Maybe eventually, but it sure doesn't—there is good evidence that it doesn't always win in the short term. And how far are we willing to go down that path? That is a very tough policy question that is way above my pay grade to answer.

Mr. FALLON. Do you believe, the panel believe, that forming an information command would be something that we should explore?

Dr. KIRSCHBAUM. Mr. Fallon, this is Joe Kirschbaum. So I am not sure a command is necessary. The reason that your question

piqued my interest is I remember more than 10 years ago, before Cyber Command was stood up, I remember having a conversation with someone in the Department of Defense, and someone asked me and said, What would be your biggest surprise after we are—eventually stand up this U.S. Cyber Command? You know, however many years from now, and I forget what they asked me. And my answer to them was, my number one surprise would be if it is still called U.S. Cyber Command, because of the nature, you know, what we are talking now, the information environment involves so much more, and cyber is a part of it.

So people have argued for, in fact, that maybe Cyber Command should be expanded. We are agnostic on that. We, obviously, don't have an opinion on that. But those are the kind of things to think about. It's, on the one hand, too broad to be just one organization, but you definitely got to make sure that everyone understands what that breadth means, and who is involved, and get them working the correct way. That is more important than establishing an organization.

Mr. LANGEVIN. Thank you very much. The gentleman's time has expired.

Mr. Khanna is recognized now for 5 minutes.

Mr. KHANNA. Thank you, Mr. Chairman. And thank you to all of the panelists for your testimony. Many of you have spoken about the importance of the United States maintaining our strategic advantage in AI and in industries of the future. I wonder if any of the panelists have followed the bipartisan effort that Senator Schumer, Senator Young, Representative Gallagher, and I [have undertaken] with the Endless Frontiers Act, which would put $100 billion over 5 years in the National Science Foundation, and create a technology directorate to make sure America is collaborating with the private sector to lead in the industries of the future, a bipartisan bill that has six Republican Senators, a number of Republicans and Democrats on in the House. And I wonder if any of the panelists have comments about the importance of that legislation?

Mr. GERSTELL. Congressman, I would simply say that that is exactly the part of the effort that we talk about when we say we need a whole-of-society effort. And the National Commission on Artificial Intelligence, to which we have made many allusions, certainly, underscore the need for a highly trained and skilled workforce. And the legislation that you just described would be a significant step in that direction.

The Office of the Director of National Intelligence in its Global Trends 2040 Report, talking about what future scenarios would look like, made great reference to the fact that it would be critically important for our country to have a really skilled workforce to be able to deal with the challenges of the digital revolution. So anything we can do in that regard is clearly going to have very significant dividends. That by itself isn't going to stop disinformation, no one suggests that it would, but it is part of the overall solution.

Mr. KHANNA. Let me ask you this: I was reading—I am going to ask two different questions. I read the report that Eric Schmidt and others did on the National Security Commission on Artificial Intelligence. So, I think one of the critical points in there is that right now, the AI traditionally has—it requires voluminous data.

But when you are a child and you are learning, let's say, the word "dog," it is not like we put give a child thousands of data points or pictures of dogs. They see a few dogs, and they learn the word "dog," which suggests that the human mind is far more complex and sophisticated than current AI. And there is work being done at MIT [Massachusetts Institute of Technology] and other places to try to understand how the human mind actually comprehends with probabilistic modeling that would allow AI to operate without voluminous data.

Could you speak to how much of a comparative advantage that would be over China, given that China has a data advantage if we are able to have AI that doesn't require as much data?

Mr. GERSTELL. I am not sure I have the expertise on that particular topic. I don't know if the other panelists do.

Dr. LIN. I know enough about that to be dangerous. So please don't take my word as gospel. It is definitely worth an inquiry. I will just point out that the Chinese are aware of this, too, and they also understand the importance of understanding the neurophysiology of the human brain.

And, so, I think that to assume that we could go down that path and the Chinese wouldn't, I think doesn't work. It is true that the Chinese have many data advantages, in some ways, and other places we have better data advantages. But to assume that the Chinese aren't aware of the importance of neurophysiology and so on in the human brain, I think is probably not correct.

Mr. KHANNA. We always have good insight. And I wasn't suggesting that China was unaware of—well, I do think leading research is being done in the U.S., but more that the data advantage that China has is enormous if we don't have alternative innovations.

The final question I have is, I don't know if any of the panelists have studied what Finland has done. I was reading somewhere that they have this extraordinary intervention at the age of 6, because the Russian disinformation campaign was a big problem there. And that this digital literacy campaign has, presumably, or at least from what I have read, worked in having a more informed citizenry that doesn't fall for disinformation. A, is that true? Are any of you familiar with the program in Finland? And, B, do you have any ideas of what digital literacy would look like in the United States?

Ms. JANKOWICZ. I am happy to take that one, Congressman. Yes, absolutely, that is true. It was not only on Comedy Central with Samantha B, but there are many academic studies of this as well. And the program starts as early as 5, actually, with students getting exposure to what is an ad versus what is your Saturday morning cartoon? So, really, not just media literacy, but general informational awareness.

And I would say the United States needs to go one step farther when we are talking information literacy. We often think about this as something that we can fairly easily, even given our federal education system, do in schools. But I would say we need to reach voting age adults as well. And how can we do that? I mentioned libraries before. Libraries maintain a very high level of trust across partisan divides in the United States. We have a lot of them. They

are looking for their raison de'être in the 21st century. And I think this is a great vehicle to deliver this sort of training.

In the Czech Republic, they have a similar program. I like to call this the peas-in-the-mashed-potatoes approach. It is targeted at elderly people, teaching them how to use their cell phones or iPads to Facetime their grandchildren, just basic computer skills. But they also sneak in some information literacy in there. And that, again, gets to the need to be creative with these sorts of approaches and think outside of—outside of our normal education national security boxes.

But the most important thing, not only having a nonpartisan messenger, but the curriculum itself needs to be nonpartisan, and make sure that we are giving the people tools that they need to support the information that they are trying to gather, to make decisions at the ballot box, to, you know, make economic decisions, et cetera. It shouldn't be motivated by any partisan agenda.

Mr. KHANNA. Well, thank you. I would look forward to working with you and maybe in a bipartisan way. I think that would be a very worthy project for the Congress, in a bipartisan way, if we can design a form of digital literacy for students and adults. And with that, Mr. Chair, I yield back my time.

Mr. LANGEVIN. Thank you, Mr. Khanna.

Mrs. Bice is recognized for 5 minutes.

Mrs. BICE. Thank you, Mr. Chairman. This is really for any of the panelists. You know, it is crucial for our Nation to have our own robust, offensive information operations capabilities in place to influence adversary actions, deceive enemies, and to try to stay ahead of the adversarial decision making in times of war. What role do you feel is proper for the military in this area?

Dr. KIRSCHBAUM. So, Mrs. Bice, the Department of Defense really—it is, at its heart, is an operational military role. So at the operational level of war, you know, it is below the strategic level. That is primarily what we have been looking at, what we are talking about. How to make sure that everyone at the combatant command level, the commander understands, as he or she is working with partners at the ambassador level, or regional allies and partners, understands what we are trying to achieve, and to get that done. So those are campaigns that we talked about that are taking place below the threshold around conflict all the time. The military has—that is the primary thing that we are talking here in terms of what the military's role is.

Now, that whole-of-government approach that bring it up a level, strategy, where does the United States fit in with its allies and partners? That is a much broader—that whole-of-government, whole-of-society. In this case, the Department should plug in to whatever efforts are being done and led out of places like the State Department or whatever organizations get created in the future. You know, during the Cold War, we had the United States Information Agency that organized a lot of those things; that orchestrated large campaigns to support information for our allies, our partners, and beyond into the Iron Curtain, for example. That is a huge undertaking that no longer exists. That is gone. That has been swept away. And we can't necessarily just recreate it, nor should we, but we think about how we do that. And the military

would plug in to those efforts in addition to maintaining its own battlefield capabilities.

Mrs. BICE. That is all I have, Mr. Chairman. I yield back. Thank you.

Mr. LANGEVIN. Very good. Is there any member on that hasn't been recognized yet that wants to be recognized?

I think we have gotten to everybody.

Okay. With that, I just want to thank our witnesses for your testimony today. It has been very insightful and very helpful to our work. I know that I had additional questions, and other members may have additional questions that we would like to submit for the record. If you could respond to those, it would be very helpful as well.

So with that, again, thank you to our witnesses. I deeply value your expertise and your contributions to this important conversation in helping us to understand and get our arms around these challenges. With that, the hearing stands adjourned. Have a great weekend, everyone.

[Whereupon, at 4:27 p.m., the subcommittee was adjourned.]

A P P E N D I X

APRIL 30, 2021

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

APRIL 30, 2021

Opening Statement
Chairman James R. Langevin
Cyber, Innovative Technologies, and Information Systems Subcommittee:
Technology and Information Warfare: The Competition for Influence and the Department of Defense
April 30, 2021

I would like to welcome the members who are joining today's remote hearing. Members who are joining must be visible onscreen for the purposes of identity verification, establishing and maintaining a quorum, participating in the proceeding, and voting. Those Members must continue to use the software platform's video function while in attendance, unless they experience connectivity issues or other technical problems that render them unable to participate on camera. If a Member experiences technical difficulties, they should contact the committee's staff for assistance.

Video of Members' participation will be broadcast via the television/internet feeds. Members participating remotely must seek recognition verbally, and they are asked to mute their microphones when they are not speaking.

Members who are participating remotely are reminded to keep the software platform's video function on the entire time they attend the proceeding. Members may leave and rejoin the proceeding. If Members depart for a short while, for reasons other than joining a different proceeding, they should leave the video function on. If Members will be absent for a significant period, or depart to join a different proceeding, they should exit the software platform entirely and then re-join it if they return. Members may use the software platform's chat feature to communicate with staff regarding technical or logistical support issues only.

Finally, I have designated a committee staff member to, if necessary, mute unrecognized Members' microphones to cancel any inadvertent background noise that may disrupt the proceeding.

With that, I will give my opening statement. Welcome to our hearing today on Technology and Information Warfare: The Competition for Influence and the Department of Defense. I want to thank Ranking Member Stefanik for joining me in holding this hearing today.

I also want to thank our witnesses for appearing today.

To discuss technology enabled information warfare as a national security threat, we welcome:

- Mr. Glenn Gerstell-Senior Advisor at the Center for Strategic and International Studies, and
- Ms. Nina Jankowicz-Disinformation Fellow at the Wilson Center

And to provide insight on the Pentagon's information operations strategy and leadership we are joined by:

- Dr. Herb Lin-Senior Research Scholar at Stanford University, and

- Dr. Joseph (Joe) Kirschbaum-Director, Defense Capabilities and Management Team at the Government Accountability Office.

Dr. Kirschbaum welcome back. And I thank you all for appearing today. This is truly an esteemed panel.

The United States is challenged in the information environment daily. Competitors like China, Russia, and violent extremist organizations use information warfare to achieve their objectives below the threshold of armed conflict as they seek to avoid traditional U.S. military advantages and undermine the free international order and democratic values.

The recently released Annual Threat Assessment of the US Intelligence Community makes clear that a variety of state and non-state actors weaponize information to undermine the United States by sowing discord among our citizens, influencing decision makers, and reversing what had once been a strength of our nation's historical information advantage.

I often focus on what lies ahead in defense, but it is worth noting that the United States and the military are facing momentous challenges in the information environment right now, which can undermine the very fabric of our democracy.

And what makes these threats particularly powerful is that foreign adversaries can target U.S. and allied citizens almost instantly without crossing physical boundaries or borders.

These threats will only grow as artificial intelligence and other technology-enabled information operations exponentially increase the speed and scope of the danger. According to the National Security Commission on Artificial Intelligence, state adversaries are employing artificial intelligence-enabled disinformation attacks to sow division in democracies and disrupt the public's sense of reality. But how to confront these national security challenges is a difficult question.

I believe the nation must respond forcefully to deter bad actors in the information domain, invest in robust U.S. public diplomacy, and educate the public and our service members about these dangers. We must also articulate a vision for the information environment and delineate thresholds of behavior that will trigger a response.

I was encouraged when the National Security Commission on Artificial Intelligence recommended that the United States develop a new strategy to counter disinformation while investing in technology to counter artificial intelligence-enabled information warfare. And I am also looking forward to the insight our witnesses will provide on how to address these threats.

Likewise, we will explore how the Department of Defense is organized to compete in the information environment, including cyber, the electromagnetic spectrum, military information support operations, deception, and operational security.

The military is challenged in the information environment by capable adversaries, and Department of Defense priorities must reflect this reality. The Pentagon has a critical role in protecting the nation, our partners, and our allies

from threats in the information environment, and in advancing our national interests in this sphere.

Recognizing this, Congress and this committee have continuously pushed the Department to prioritize adapting to the weaponized information environment, including by creating the Principal Information Operations Advisor. Yet, I am concerned the Department leadership has been slow to adapt to the changing nature of warfare in this domain.

To give an example, in 2020, 9 of the then 11 four-star combatant commanders wrote a memorandum asking for additional support for their information operations. They wrote, quote, "We continue to miss opportunities to clarify truth, counter distortions, puncture false narratives, and influence events in time to make a difference."

Too often, it appears the Department's information related capabilities are stove-piped centers of excellence with varied management and leadership structures, which makes critical coordination more difficult. Further, the Pentagon has made limited progress implementing its 2016 Operations in the Information Environment Strategy, which raises questions about the Department's information operations leadership structure.

These are challenging questions without easy answers. But I hope my colleagues will take advantage of the impressive array of witnesses we have before us today.

I'll now turn to Ranking Member Stefanik for her remarks.

Statement of Glenn S. Gerstell*

Before the Subcommittee on Cyber, Innovative Technologies, and Information Systems of the U.S. House of Representatives Committee on Armed Services

Hearing on Technology and Information Warfare: The Competition for Influence and the Department of Defense
April 30, 2021

A thoughtful book about the digital age observed that as people spend more and more time in cyberspace, the growing power of the internet "will make everything different: power shifting away from the center toward individuals and small organizations, more fluidity and continuous change, increasingly irrelevant national boundaries." The internet will give individuals "the ability to be heard across the world…along with the ability to spread lies worldwide…and will foster decentralization…undermining central authorities whether they are good or bad."

While we would recognize that as a description of our cyber world today, these prescient statements appeared 24 years ago, in Esther Dyson's *Release 2.0* – written in 1997, before the invention of Facebook, YouTube or the iPhone.

I mention this quotation because we need some perspective or sense of distance to appreciate the ramifications of the digital revolution, or the "Fourth Industrial Revolution." We tend to view both the exceptional benefits of technology and the negative consequences in isolation, looking at each new function and drawback as a separate, unrelated event, marveling at how we can now control our garage doors from halfway around the world, or worrying about cyber ransomware attacks on hospitals. But in this onrush of both innovation and mischief, we do not fully appreciate the fundamental, novel and transformational changes that we are in the midst of – and these changes have national security implications.

Technology has Yielded New Vulnerabilities Threatening our National Security

There are three related implications of these technological changes that our nation – and in particular this Subcommittee – must consider. First, our overall domestic wellbeing is, for the first time since America became a global power, directly threatened by what happens beyond our shores. Second, our wellbeing, in other words, our national security, is now partly the responsibility of the private sector, not just government. And the third point, which I will concentrate on today, is that the cyber-enabled spread of disinformation on the private sector's social media platforms is altering our political landscape, threatening democracies and global coordination.

---

* Glenn S. Gerstell served from 2015 to 2020 as the General Counsel of the National Security Agency and is currently a non-resident Senior Adviser at the Center for Strategic and International Studies. Additional background at https://glenngerstell.com.

Let's take the first and most obvious of these changes – the risks to our national security posed by other countries. Historically, when we think about this kind of vulnerability, we have thought of it as a threat posed by other nations' weapons; we rightly spend a great deal of time and money deterring or defending against those dangers. For over two centuries America has responded to foreign threats by dealing with them where they were located, in other words, overseas -- not allowing them (with the sole exception of the 9/11 attacks) to manifest themselves on our domestic soil. But as we've seen recently – due to technology – a virus that can be propelled around the world, and cyber mischief that is equally oblivious to sovereign boundaries, can have a devastating effect on our personal and commercial lives. While we must of course remain vigilant about the risk of another nation's weapons injuring us on our soil, we are far more likely to be harmed by other technology-propelled dangers emanating beyond our borders.

Or to put it in a more serious way, due to technology, our overall national wellbeing – our national security – is for the first time challenged by, and vulnerable to, other countries in ways that we will have difficulty managing, since these other threats are not deterred or blocked by our superior military strength.

These new vulnerabilities do not reside in weapons systems, but instead pervade our private sector. With responsibilities for cyber-safeguarding its vast troves of data about our personal and commercial lives and for stemming the tide of disinformation on the social media we all rely on for our news, the private sector clearly bears critical national security burdens. We rely on the private sector to a degree unthinkable just a decade or two ago: even at its heyday, a problem at General Motors wouldn't have affected our national wellbeing, but today, a mishap at Google or Facebook or a disruption at Amazon or Microsoft (together responsible for almost half of the nation's cloud computing capacity) might well cause deep disruptions to our society. In short, as the recent *Final Report* of the National Security Commission on Artificial Intelligence (NSCAI) succinctly stated: "Digital dependence in all walks of life is transforming personal and commercial vulnerabilities into potential national security weaknesses."

We focus less on these vulnerabilities, for many reasons. First, we don't typically think of the private sector as responsible for national security. It used to be clear that only government was responsible for national security, or the "common defense" as the American Constitution calls it, and our private sector was largely free to pursue its business goals, and the lines between the two were pretty clearly delineated. But the digital revolution has shifted those lines, and in many ways, for the first time in our nation's history, our national security increasingly rests not with the federal government but instead with a private sector that conducts our digital lives. Second, even when there are problems with private sector technology, we typically view them as incidents confined to one company, not signs of systemic risk to our country. Finally, and more significantly, the enormity of the ongoing shift of responsibilities to the private sector is difficult to embrace.

Online Disinformation is the Most Pernicious of those Vulnerabilities

Some of those technological mishaps could simply be technical failures to provide service, but in the area of information technology, problems affecting the substance of communications can be equally consequential. And that takes us to the third transformational consequence: the

advent of disinformation on domestic social media platforms. Perhaps the most pernicious aspect of the digital revolution, disinformation threatens our very democracy. By disinformation, I am referring to the deliberate (or at least reckless) creation or dissemination of knowingly false (or at least baseless) information, with an intention to mislead the reader or viewer; the goal might be a specific effect or simply a more diffuse confusion or chaos. While the line might be hard to draw, it's clearly more than a spoof or simply erroneous information.

Esther Dyson's prescient vision has indeed come to pass. The fact that the internet gives everyone a potentially equal megaphone – whether you are the *Washington Post* or a white supremacist blogger – means that the lines between establishment news sources and unreliable ones are blurred. So with no curated and vetted sources of information, without elites more or less shaping the flow of the news, anything goes – and it does. Human nature being what it is, we are drawn to the more lurid, improbable or conspiratorial, at least to explain what might not be apparent or understandable. So rather than being an unalloyed good for democracies, it turns out that chat and other online platforms are a fertile ground for populism, divisiveness and political disintegration. Admittedly, it's not wholly negative and there are many examples where the ability of individuals to obtain and disseminate information has worked against authoritarian regimes; but my point is simply that – absent safeguards – the technology seems to easily lend itself to bad outcomes.

Over the past few months, as we've seen in detailed reports from many organizations, including the Alliance for Securing Democracy, Avaaz, Graphika and The New York Times, those platforms have been awash in falsehoods on political topics ranging from election fraud, to the Capitol insurrection, to climate change and to Antifa protestors. When you stop to think about it, it's quite extraordinary that we are now more worried about the private sector, which owns Facebook, Twitter, YouTube, Instagram and the other popular platforms, shaping and influencing what we think. America was founded in part on concerns that the government might control what we think and believe, and while that remains an enduring concern, the reality is that our domestic wellbeing is threatened far more by private sector social media polluted by falsehoods.

It can't be healthy for a democracy when almost half the population wasn't sure if our president was duly elected, and more shockingly, that only four in ten Americans thought the recent election was fair and accurate. At least in the case of elections and political speech, disinformation has a corrosive effect on democracy, leading to mistrust of institutions, cynicism about our leaders and skepticism about our ability to solve social problems, and ultimately raising the specter of authoritarianism as a reaction to that corrosion. Indeed, one of the key trends identified in the just-released *Global Trends 2040* report from the Office of the Director of National Intelligence was that online technologies would continue to foment and channel public discontent – yielding a deeply disturbing picture "with a mix of implications for social cohesion."

But disinformation is affecting not merely our political institutions. When three out of four Americans get some or all of their news from social media platforms, it is clear that the risk of deliberately incorrect online information is national in scope, and could get worse. A recent Gallup poll revealed that, due to erroneous fears spread on social media about the safety of COVID vaccines, roughly a third of the country has doubts about getting a shot, and many others

refuse to follow the advice of doctors and scientists and wear face masks, choosing instead to believe false online claims that masks are useless. So even a seemingly non-partisan sphere such as public health can be politicized and damaged by cyber-disinformation.

Beyond threats to the fundamentals of our democracy and our public health, disinformation could affect our military in concerning ways. At the most general level, the cynicism about our institutions and mistrust of political leaders endangers the national consensus that we must devote sufficient resources to our armed services. It stands to reason that a lack of trust in our military might well threaten public support for Congressional appropriations for weapons systems or veterans affairs and more directly, recruiting for our all-volunteer military forces. And speaking of personnel, it isn't much of a stretch to attribute, at least to some degree, extremism in the military to the effects of malicious lies spread online. Although it is beyond my scope today, information warfare in armed conflict is obviously a threat to service personnel morale, command and control of forces, and relations with local populations in the area of operations. Indeed, recent press reports indicate that senior military leaders are seeking closer cooperation with the US Intelligence Community to help counter malign influence campaigns of Russia and China.

These concerns about disinformation are not just idle speculation. Just a few months ago, the Reagan Institute survey revealed that, after several politically turbulent years, citizens' trust and confidence in our military dropped to just 56%, down from 70% as recently as 2018. Even more shocking was the finding that levels of trust in institutions from law enforcement to public schools to the news media and the presidency and Congress were all below 50% of the population. How much of that is attributable to online disinformation? There's no way of knowing, but common sense tells us that the manifestly corrosive effect of such disinformation must be a key element in this societal disintegration.

Broader threats to our military arise from a world situation in which our foreign adversaries use disinformation as a tool of their statecraft. Lies fomented by our overseas foes about foreign affairs and our vital interests abroad could similarly make cooperation with our allies and friends more difficult. For example, China's concerted online campaign to deflect investigations into the cause of the COVID19 outbreak, to paint themselves as successful in curtailing the virus when Western democracies have been foundering, and to deny their militarization of the South China Sea, all complicate if not undermine our foreign relations, and heighten the chance for conflict. The combination of disinformation and the difficulty of promoting a concerted establishment message have all hampered efforts at, or at least made it more difficult to achieve, global cooperation on a variety of matters. All of these geopolitical consequences, with their myriad and complex effects, are the product of a technology in which electrons are ignorant of sovereign boundaries.

Foreign-Generated Disinformation is Likely to Get Worse

Recent events have caused us to focus mostly on domestic disinformation in somewhat contained (albeit critical) channels, and on the relatively limited efforts of our foreign adversaries to undermine our democracy and promote their governing systems over our own. For both technical and political reasons, however, the effects of cyber-propelled disinformation are likely to get much worse; we would have difficulty in fending off weaponized disinformation coming

from a sophisticated foe. As the five-volume bipartisan report of the Senate Select Committee on Intelligence on the 2016 elections clearly illustrated, Russia availed itself of the open and unquestioning nature of social media platforms to create fictitious online personas to spread falsehoods about the presidential election, and recycled their fabrications through controlled spurious news sites to corroborate and amplify their disinformation. So we have seen what a sophisticated adversary can do in a focused area such as election influence, but there's no reason to think their playbook couldn't be greatly expanded.

On the technical side, the advent of 5G wireless communications and essentially ubiquitous smart phone use mean that virtually everyone will have instantaneous access to information, both accurate and inaccurate, and the deployment of artificial intelligence in an integrated way in communications systems has the potential for shaping and micro-curating news feeds. Referring to a "gathering storm of foreign influence and interference," the NSCAI *Final Report* notes that "adversaries are using AI systems to enhance disinformation campaigns....They are harvesting data on Americans to build profiles of their beliefs, behavior, and biological makeup for tailored attempts to manipulate or coerce individuals." Moreover, increasingly sophisticated AI systems will enable the rapid creation of probably undetectable deep-fake videos and audio recordings, with rich potential for malice and immediate effect. The result might be a world in which we are suspicious of any communications that we cannot authenticate ourselves. While that skepticism might limit the believability of deep-fake videos, such suspicion would surely extend equally to "official" news sources, yielding a chaotic and unreliable reality in which truth and genuine information are elusive.

The seemingly inexorable trajectory of foreign cyber hacks and attacks is instructive for predicting the future of online disinformation from our adversaries. Over the years, Russia, China, Iran and North Korea have all incrementally stepped up their cyber maliciousness, as new vulnerabilities come into existence, ever-more sophisticated tools are created to exploit them, and hacks and attacks succeed again and again without any serious repercussions to the wrongdoers. Operating just below the threshold of war, our cyber rivals can, for a variety of reasons, mostly act with impunity. The same factors that shield those foes in hacks and attacks – the uncertainty of provable attribution, the absence of directly caused actual injury or physical damage and other factors – also will insulate them as they inevitably step up their disinformation campaigns. Indeed, as disinformation is more diffuse in its effect and can be cloaked as mere opinion, it can be wielded with even less concern for retribution. It's hard to see why those adversaries will in the future limit themselves to election influence – little is standing in the way of general commercial disinformation (say, questioning the safety of Boeing aircraft) or undermining our governmental system (for example, asserting that jury trials are rigged, or that municipal water supplies aren't properly maintained).

More specifically, what if Russia or Iran seizes on a real natural disaster – say, a hurricane or flood – and weaponized the crisis with false information online, amplifying and corroborating it on their controlled news sites, and fed false information about the hurricane's path or expected river crestings or even wrong instructions about escape routes? In the future, a coordinated disinformation attack on multiple platforms, especially one seizing on an urgent public safety problem or an already contentious issue such as vaccine safety, could provide the kind of apparent corroboration that would lead to chaos, and it could take weeks – if ever – for the truth to be broadly accepted. What if days before the next election, a deep-fake video

manufactured by Russia's intelligence services – virtually undetectable as a fraud – goes viral on YouTube purporting to show a Congressional candidate having a sexual liason with a minor?

Starting to Fix the Problem

We know disinformation is already a big problem, and we fear it could be even worse, so why haven't we done something about it? As with any complex problem, there are many answers. First, like other bad side effects of our cyber lives, there's no miracle drug to cure this disease. Second, we've historically taken a minimal and reactive approach to regulation of the private sector, and even if we started to draw up laws to deal with it, disinformation has itself become a paralyzing political issue. Besides, we're uncomfortable with regulating any speech, and it's not really obvious what we can do about the problem anyway, so we just throw up our hands. As long as disinformation is just gradually corroding our institutions or hindering our national political will or insidiously prolonging a pandemic, there's no one day that we must fix the problem.

We could wait until a crisis or disaster. But we don't need to. The very fact that there are many sources contributing to disinformation means that we have multiple ways to stem it. There are steps we can take to start to fix the problem. No one solution is at hand, but we have tools at our disposal to use and they will, bit by bit, make a difference. I'll mention just three that will help attenuate the threats to our national security.

Probably the most obvious tool is the law, but we first have to get over what seems like a big obstacle. We want neither government nor the private sector to be the final arbiter of the truth or the decider of what we hear and see. Yet allowing the private sector to profit from manipulating what we view online without regard to its truthfulness or the consequences of viral dissemination is simply not sensible public policy. But it's not all or nothing, there is room for some thoughtful regulation. After all, the First Amendment applies only to government and not to private businesses.

So there's room for Congress to act in tightening rules on political campaign ads, perhaps by making certain knowing or intentional falsehoods illegal, such as deliberately spreading incorrect information about polling places – much in the way that the law prevents someone from filing a false police report. Admittedly, there is a delicate line between a prank or spoof, and something clearly malicious and potentially illegal. But the mere fact that the line may be difficult to draw, need not preclude legislation that provides a framework for that process. As has been the subject of recent Congressional attention, some amendment of Section 230 of the Communications Decency Act could be helpful. However well-intentioned at the time of its adoption, the law has come to insulate the business models of social media platforms that are the source of information for billions of people around the globe. These ad-driven models rely on secret, complex algorithms that micro-target users, facilitating the forwarding of material without regard to its accuracy, thus allowing falsehoods to go viral, and often amplifying problematic material.

Another obvious tool is the technology itself. The very technology that helps spawn the problem can be used to correct it too, with AI helping social media platforms spot lies in the first place, identify doctored videos and photographs, and track the dissemination of falsehoods by

both domestic and foreign users. And after social media was awash in disinformation during the pandemic and this last election, the platforms finally abandoned their hands-off approach and were more muscular in blocking objectionable content and taking down sham or malevolent accounts. True, there will always be difficulty in deciding what's sufficiently objectionable or incorrect to warrant labeling or even removal – but again, just because it's tough to draw the line doesn't mean we shouldn't even start. One helpful step would be for greater transparency about how such decisions are made, and how a platform's algorithms make recommendations and curate what we see and hear.

Finally, there's a whole range of other steps that can be taken beyond regulation of social media platforms. For example, we could promote international coordination to stop the export of disinformation or to bring cross-border cyber criminals to justice. We could do a much better job of organizing our federal government in a coherent way to fight disinformation, perhaps by setting up a national disinformation center within our intelligence community, just the way we've successfully done with the national counterterrorism center. The Intelligence Community could work more in a more integrated way with the military to counter adversaries' ongoing malign influence campaigns. Saving the potentially most profound step for last, we would garner rich benefits by teaching digital literacy and putting civic education back in our schools – so that disinformation, whether foreign or domestic, will be less likely to take hold in an educated and cyber-sophisticated populace.

Addressing the Threat of Disinformation Is Difficult but Necessary

Cyber-enabled disinformation, whether domestically or foreign generated, is a national security problem, corroding our democracy and governmental institutions, and threatening our public health and, potentially, public safety. It presents special challenges to our military, both because our armed forces are one of those governmental institutions whose credibility is at stake, and because the military obviously plays a unique role in assuring our national security. Those challenges are likely to get worse, with the ongoing march of technology and increasing willingness of our foreign adversaries to use the tool of disinformation to advance their interests. Responding to these challenges will not be easy, since it will require making difficult and controversial decisions about the responsibility of the private sector for our national wellbeing and about restrictions on speech.

Differing ideas are inherent and indeed necessary in any democracy, and there is always fertile ground for discord. But when that discord is polluted by disinformation – whether maliciously homegrown or skillfully fomented by foreign adversaries – it is difficult for government alone to respond. Congress should lead the way, but in the end it is up to our society to come together to manage the increasing cyber vulnerabilities of our everyday personal and business lives. Our national wellbeing depends on nothing less.

Thank you for the opportunity to present my views to the Subcommittee.

Glenn S. Gerstell
Senior Adviser (Non-resident), International Security Program

ASSOCIATED PROGRAMS: International Security Program

Glenn S. Gerstell served as the general counsel of the National Security Agency (NSA) and Central Security Service (CSS) from 2015 to 2020. He has written and spoken widely about the intersections of technology and national security and privacy. Prior to joining the NSA, Mr. Gerstell practiced law for almost 40 years at the international law firm of Milbank, LLP, where he focused on the global telecommunications industry and served as the managing partner of the firm's Washington, D.C., Singapore, and Hong Kong offices. Mr. Gerstell served on the President's National Infrastructure Advisory Council, which reports to the president and the secretary of homeland security on security threats to the nation's infrastructure, as well as on the District of Columbia Homeland Security Commission. A graduate of New York University and Columbia University School of Law, Mr. Gerstell is an elected member of the American Academy of Diplomacy and a member of the Council on Foreign Relations. Earlier in his career, he was an adjunct law professor at the Georgetown University Law Center and New York Law School. He is a recipient of the National Intelligence Distinguished Service Medal, the Secretary of Defense Medal for Exceptional Civilian Service and the NSA Distinguished Civilian Service Medal.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the House of Representatives for the 117th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), and contracts or grants (including subcontracts and subgrants), or payments originating with a foreign government, received during the past 36 months either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. Rule 11, clause 2(g)(5) also requires nongovernmental witnesses to disclose whether they are a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing. As a matter of committee policy, the House Committee on Armed Services further requires nongovernmental witnesses to disclose the amount and source of any contracts or grants (including subcontracts and subgrants), or payments originating with any organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months either by the witness or by an entity represented by the witness. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number), will be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary. Please complete this form electronically.

Hearing Date: April 30, 2021

Hearing Subject:

Technology and Information Warfare: The Competition for Influence and the Department of Defense

Witness name: Glenn S. Gerstell

Position/Title: Senior Adviser (Non-resident), International Security Program, Center for Strategic and International Studies

Capacity in which appearing: (check one)

● Individual ○ Representative

If appearing in a representative capacity, name of the organization or entity represented:

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
n/a			

2020

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
Grant	Department of Homeland Security	$85,010.30	Public Acceptance of Facial Recognition Technologies
Contract	Defense Threat Reduction Agency	$141,944.00	Scenarios on the Future Threat Environment
Grant	Defense Innovation Unit	$99,900.00	National Security Innovation Base (NSIB)
Grant	Department of Homeland Security	$85,010.30	Public Acceptance of Facial Recognition Technologies

2019

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
Grant	Naval Postgraduate School	$120,000.00	Industrial Mobilization - Assessing Surge Capabilities, Wartime Risks, and System E
Grant	Department of State	$395,000.00	Strengthening International Engagement on Security in Cyberspace
Donation	U.S. Army Future Commands	$1,500.00	Army Future Studies Group engagment

2018

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
n/a			

Foreign Government Contract, Grant, or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants), or payments originating from a foreign government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
Grant	Department of Foreign Affairs and Trade, Australia	$33,333.33	Roundtable Series: Exploring a Menu of Consequences for Malicious Cyber Actions
Donation	Japan External Trade Organization (JETRO)	$25,000.00	5G National Strategy
Grant	Ministry of Foreign Affairs Estonia	$35,559.30	Roundtable Series: Exploring a Menu of Consequences for Malicious Cyber Actions

2020

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
Donation	Japan External Trade Organization (JETRO)	$25,000.00	5G Supply Chain Risk Management
Grant	Cyber Security Agency of Singapore	$12,500.00	Inside Cyber Diplomacy

2019

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
Donation	Japan External Trade Organization (JETRO)	$40,000.00	China Innovation Policy Series
Grant	Government Of Canada	$36,011.86	Principled approaches to hybrid warfare

2018

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
Donation	Ministry of Economy, Trade and Industry (Japan)	$40,000.00	5G supply chain security

Fiduciary Relationships: If you are a fiduciary of any organization or entity that has an interest in the subject matter of the hearing, please provide the following information:

Organization or entity	Brief description of the fiduciary relationship
n/a	

Organization or Entity Contract, Grant or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants) or payments originating from an organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months, please provide the following information:

2021

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
n/a			

2020

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
n/a			

2019

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
n/a			

2018

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
n/a			

Statement of

NINA JANKOWICZ

Woodrow Wilson International Center for Scholars

Science and Technology Innovation Program

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES

ARMED SERVICES COMMITTEE

Subcommittee on Cyber Innovative Technologies and Information Systems

Concerning

"Technology and Information Warfare:
The Competition for Influence and the Department of Defense"

April 30, 2021

Chairman Langevin, Ranking Member Stefanik, and distinguished Members of the subcommittee, thank you for the opportunity to discuss technology, information warfare, and the competition for influence with you.

I am the daughter of a veteran. My father—an aerial reconnaissance officer in Vietnam—died in 2010 after complications from multiple myeloma, which he contracted as a result of his exposure to Agent Orange during his service. I know he would be thrilled to see me testifying before this committee in the service of truth.

I have spent my career on the front lines of the information war. I worked on Russia and Belarus programs at the National Democratic Institute, a target of authoritarian information operations (IO) including from Moscow and Beijing. Under a Fulbright Public Policy Fellowship, I advised the Ukrainian Ministry of Foreign Affairs on strategic communications. I spent the last four years researching how our allies in Central and Eastern Europe dealt with Russian online aggression long before the United States even recognized it as a threat.[1]

Since I began studying this topic, I have observed incremental improvements in the way social media companies, the press, the American people, and government have responded to the threat of disinformation. Now, at least, we seem to all recognize the threat *exists*. But as I told your colleagues on the Appropriations Committee at a 2019 hearing on responding to disinformation, "the United States has been a tardy, timid, or tertiary player...stymied by domestic politicization."[2]

Unfortunately, the same conclusion holds true today, nearly two years later. So it also bears repeating: **disinformation is not a partisan issue. As we witnessed throughout the COVID-19 pandemic and especially on January 6, it is a democratic one, affecting public health, public safety, and the very processes by which the United States is governed.** It is critical that Congress understand this; otherwise, we remain vulnerable to information warfare, and the policy changes I am recommending today cannot be successful.

How did we get here? In part, our understanding of the problem is to blame.[3] Since the end of the Cold War and the resurgence of great power competition, the United States has conceptualized hostile-state information operations as one-off occurrences—explained away by societal peculiarities, tensions, and events such as elections—that warrant attention only in the moment. Rather than organizing cross-cutting, proactive, whole-of-government responses, we have mostly stood up ad hoc capabilities only when necessary, such as election war rooms before events like the 2018 and 2020 elections.

Furthermore, US government efforts to counter information operations have been largely securitized, primarily involving elements of the Defense, Homeland Security, and State Departments, in addition to

---

[1] Nina Jankowicz, *How to Lose the Information War: Russia, Fake News, and the Future of Conflict* (London: Bloomsbury/IB Tauris, 2020).

[2] Nina Jankowicz, Testimony before the House Appropriations Committee, State and Foreign Operations Subcommittee, July 10, 2019.

[3] Adapted from Nina Jankowicz and Henry Collis, "Enduring Information Vigilance: Government after COVID-19," *Parameters* 50, no. 3 (2020).

the Intelligence Community. They rarely focus on building broader resilience. Even within the national security establishment, there is too little recognition of the need to shore up domestic vulnerabilities as part of a winning Counter-IO strategy.

Russia, China, and other authoritarian states, however, know these vulnerabilities are the key to gaining ground in the information war. **Adversaries like Moscow and Beijing utilize an integrated approach to information operations** and take advantage of American inaction on the issue. They have recognized the utility of engaging in **"perpetual information competition,"** which has three main characteristics:[4]

1. They understand **information competition is the new normal and are constantly probing for and exploiting societal fissures**. We have observed this in the past year as both countries amplified conspiracies about the origins of the COVID-19 pandemic and the efficacy of Western-made vaccines.[5] Russian Internet Research Agency (IRA) employees were instructed to instigate "political intensity" by "supporting radical groups, users dissatisfied with [the] social and economic situations and oppositional social movements."[6] Their accounts have pushed the Qanon conspiracy theory and augmented racial tensions around the Black Lives Matter movement in the United States.[7]

2. They **use all channels available—government and nongovernment, online and offline—to engage in this behavior**. China, for example, has utilized the "three warfares"—public opinion or media warfare, psychological warfare, and legal warfare—to shape international opinion since 2003. A wide range of state bodies—not just the traditional national security sector—are involved in China's efforts to influence and discreetly assert political power over competitors. The Ministry of Education leads efforts to instrumentalize the large number of Chinese students studying overseas, the Ministry of State Security runs fake think tanks and uses academic bodies to influence discourse, the United Front Work Department leverages the Chinese diaspora for political purposes, and the Ministry of Foreign Affairs, among others, uses targeted advertising and social media to promote the CCP position abroad.[8] This has included efforts to influence Western opinions about the protests in Hong Kong,[9] and, more recently, campaigns likely connected to the CCP attempting to paint a positive picture of life in Xinjiang.[10]

3. Finally, they know that **perpetual information competition does not adhere neatly to international borders, but rather exploits them, attempting to undermine the unity of**

---

[4] Jankowicz and Collis, 18.

[5] Bret Schafer et al, "Influence-enza: How Russia, China, and Iran Have Shaped and Manipulated Coronavirus Vaccine Narratives," Alliance for Securing Democracy, March 6, 2021.

[6] United States v. Elena Alekseevna Khusyanynova, 1:18-MJ-464 (E.D. Va 2018), 24.

[7] Ben Collins and Joe Murphy, "Russian troll accounts purged by Twitter pushed Qanon and other conspiracy theories," NBC News, February 2, 2019.

[8] Peter Mattis, "China's Three Warfares in Perspective," *War on the Rocks*, January 30, 2018; and Amy Searight, "Countering China's Influence Operations: Lessons from Australia," Center for Strategic and International Studies, May 8, 2020.

[9] Katie Paul and Elizabeth Culliford, "Twitter, Facebook accuse China of using fake accounts to undermine Hong Kong protests," *Reuters*, August 19, 2019.

[10] Raffi Khatchadourian, Twitter Post, April 23, 2021, 10:53 AM.

alliances and international organizations. Many of Russia's information operations, especially those targeting Ukraine's aspirations to join the Euro-Atlantic community, seek to denigrate Western political and military alliances, such as NATO, the European Union, and even the OSCE, of which Russia is a member. In 2016, when Ukraine sought to ratify an Association Agreement with the European Union, Russia saw an opportunity to undermine both Ukraine's EU aspirations and the European Union's cohesion by influencing the discourse about the Agreement in the Netherlands, which held a referendum on its ratification. Through fabricated videos,[11] alleged funding of fringe political movements,[12] state-sponsored propaganda, and the use of government-organized NGOs to launder information, Russia exploited and amplified Dutch citizens' unfavorable opinions about the EU and Ukraine.[13] Ultimately, voters rejected the Association Agreement and Ukraine was forced to find a diplomatic solution to get it ratified.

In these examples alone, we have observed hostile states engaged in muddying authentic discourse, influencing the outcome of elections and referenda, and pitting Americans against one another. These operations *increase* domestic tension and *decrease* American resilience, our capacity to protect our national security, and our ability to respond to foreign policy and defense policy crises.

To meet the challenge of perpetual information competition, the Department of Defense and broader United States Government should organize themselves around a posture of **Enduring Information Vigilance.** This framework sets out how the USG, through the "three Cs"—capability building, inter-office and interagency coordination, and international cooperation—can work more effectively to detect the vulnerabilities that adversaries exploit, manage those attempts, and ultimately deny adversaries any benefit.[14]

1. **Capability: Beyond Discrete Campaigns**
   In ensuring that the DoD workforce is capable of proactively monitoring and identifying informational vulnerabilities that U.S. adversaries might use in information operations, the old military adage "don't operate the equipment, equip the operator" is prescient. Tools for detecting online campaigns and inauthentic activity have developed rapidly in recent years, and parts of the national security infrastructure have adopted them, but none of these tools is a panacea without skilled staff and a baseline of resilience in the general population.

   Enduring Information Vigilance relies on skilled people with a nuanced understanding of the threat who are capable of applying the full range of tools and techniques for monitoring, detecting, and responding to information operations. Section 589E of the 2021 NDAA, which "establish[es] a program for training members of the Armed Forces and civilian employees of the Department of Defense regarding the threat of foreign malign influence campaigns targeted at such individuals and the families of such individuals, including such campaigns carried out through social media" is an excellent starting point for these efforts, given that active-duty

[11] Bellingcat, "Behind the Dutch Terror Threat Video: The St. Petersburg "Troll Factory" Connection," Bellingcat Website, April 3, 2016.
[12] Eline Schaart, "Dutch far-right leader Baudet had ties to Russia, report says," *POLITICO Europe*, April 17, 2020.
[13] Jankowicz, *How to Lose the Information War*, 123-153.
[14] Jankowicz and Collis, 27.

personnel and veterans have both been targets of state-sponsored information operations in the recent past;[15] veterans were also a key contingent among those who stormed the Capitol on January 6.[16] As this program is implemented, it is critical that training is produced together with nonpartisan subject matter and pedagogical experts and is engaging and well-resourced. This broad-based training, which would reach the 2.75 million active-duty, reserve, and civilian employees of the Department of Defense, and could also be rolled out to all civil servants and their families across the Federal Government; a bill providing for such a program is being spearheaded by the Task Force on Digital Citizenship and the Office of Congresswoman Jennifer Wexton.

Beyond such a broad resilience-building program, it is critical to equip specialists with the training and tools they need. The National Security Commission on Artificial Intelligence (NSCAI) suggests the establishment of a "Digital Service Academy to train current and future employees,"[17] though other nations' efforts suggest such training need not be relegated to a standalone body. Instead, a more agile and responsive training program might be integrated into employees' regular professional development activities. U.S. allies have adopted a similar approach; The UK Government trains its public-sector communications personnel on the "RESIST" toolkit, which emphasizes the importance of understanding the objectives of information operations when formulating appropriate responses.[18] Critically, the toolkit points out:

The speed and agility of your response is crucial in countering disinformation. This can mean working to faster deadlines than is usual and developing protocols for responding that balance speed with formal approval from senior officials.[19]

This is not DoD—or the Federal Government's—strong suit. Proactive, creative communications are often stymied and stifled by government clearance processes, resulting in ineffective and even embarrassing products that have little chance at countering sometimes-slick adversarial operations.[20]

2. Coordination: All Sectors, At All Times

The breadth of activity related to hostile state information operations, whether Russian campaigns or China's "three warfares" approach, spans the remit of multiple government agencies. The Department of Defense and wider USG must break out of siloed national security thinking, coordinate more effectively, and provide space for cross-sector cooperation. From hard security and defense to cultural activity and media, as well as many other realms of society not typically

[15] Kristofer Goldsmith, "An Investigation into Foreign Entities Who Are Targeting Troops and Veterans Online," Vietnam Veterans of America, September 17, 2019.
[16] Tom Dreisbach and Meg Anderson, "Nearly 1 In 5 Defendants In Capitol Riot Cases Served In The Military," NPR, January 21, 2021.
[17] National Security Commission on Artificial Intelligence, "Final Report," NSCAI, 2020, 127.
[18] UK Government Communications Service, "RESIST Counter Disinformation Toolkit," Government Communications Service, 2020.
[19] *Ibid.*
[20] Matthew Gault, "Read the Pentagon's 20-Page Report on Its Own Meme," *VICE News*, March 23, 2021.

situated at the forefront of foreign interference, hostile states have the potential to exploit the government's difficulty to work effectively across traditional departmental boundaries. This "bureaucratic vulnerability" can lead to poor information flow, competition for resources and influence, or the exclusion of key stakeholders.[21]

These shortcomings emphasize the need to work more effectively across government. Newly built capabilities required for monitoring, detecting, and understanding the multiple elements of hostile information activities must be integrated to advance a shared view of what adversaries are doing, whom they are targeting, and whether these activities are effective.

In its report, the NSCAI recommends the creation of a Joint Interagency Task Force bringing together the Departments of "State, Defense, Justice, and Homeland Security, and the [Office of the] Director of National Intelligence to stand-up an operations center to counter foreign-sourced malign information...survey the landscape of relevant public and private actors, coordinate among them, and act in real time to counter foreign information campaigns."[22]

While I agree with the NSCAI's conclusion that the Federal Government requires a central node for the monitoring and coordination of intelligence and policymaking around disinformation, ideally in the White House, my research across Central and Eastern Europe suggests it is necessary to involve nontraditional security departments via leads with the necessary security clearances in such efforts as well. Building this situational awareness across the government will enable the prioritized coordination of effective responses in the short term and beyond. Policy and operational levers for ameliorating vulnerabilities and building resilience against information threats in the long term lie with departments of education, health, and at local levels; they require policies that ensure a thriving and pluralistic media, societal awareness of the threat, robust media and digital literacy, and an understanding of civics.[23]

3. **Cooperation: International Partnership**

Hostile influence activities have never occurred at such a scale before. Any deterrent effect of Enhanced Information Vigilance is augmented by demonstrating resolve and denying benefit to adversaries through a collective stance against their activities, including better sharing of information and knowledge to identify threats, tactics, and tools, and the formulation of effective responses. In the wake of the attempted assassination of Sergei Skripal in the United Kingdom in 2018, the coordinated expulsion of over 140 Russian diplomatic personnel from allied nations demonstrates how a well-coordinated response can impose costs on a threat actor. Building cross-border resilience and reducing vulnerability to deny benefit, however, requires enduring cooperation and demonstrations of shared capability and resolve.

The NSCAI suggests that one way to build this resolve is through an international task force to counter and compete against disinformation, led by the Global Engagement Center (GEC) at the

[21] European Center of Excellence for Countering Hybrid Threats, "Tackling the Bureaucratic Vulnerability: An A to Z for Practitioners," European Center for Countering Hybrid Threats, 2020.
[22] National Security Commission on Artificial Intelligence, 274.
[23] Nina Jankowicz, "The Disinformation Vaccination," *Wilson Quarterly*, Winter 2018.

Department of State.[24] In principle, this is an operable suggestion, though I would add some nuance to its implementation. To begin with, the GEC's remit is too large, budget too small, and reputation within the interagency and international community too uncertain to add such a task force to its portfolio. Currently, the GEC conducts open source intelligence analysis in addition to its coordination, policymaking, and programmatic work. I recommend that intelligence gathering and analysis be left to the Intelligence Community and shared within the interagency. While the GEC should benefit from such analysis, its limited resources are better allocated in coordinating with embassies and other agencies in establishing and implementing policy and program priorities.

Finally, while the idea of a task force for international coordination is a noble one, the United States must be careful not to reinvent the wheel in its desire to engage on issues related to information operations. We are arriving late to this party and should seek to use American convening power to augment, not upstage, existing task forces and coordination efforts, particularly those spearheaded by close allies, such as the International Partnership for Countering State-Sponsored Disinformation (led by the United Kingdom in cooperation with the GEC) and the G7 Rapid Response Mechanism (led by Canada).[25]

Enduring Information Vigilance cannot be built overnight; it requires a long-term commitment that will likely outlast the political class initiating it. But the result will be a more resilient society that reassures its populations and denies adversaries benefit, deterring malign attempts to exploit the openness of democracy.

It bears repeating that our democratic values are at the core of Enduring Information Vigilance. Adversaries use information operations to exploit open societies and undermine these shared values; therefore, they must remain the center of gravity for any approach to countering hostile interference. Preserving our transparency, openness, and commitments to freedom of expression and human rights will ensure the United States continues to provide an alternative to authoritarian regimes. **We must act not only as the staunchest defender and guarantor of these values among our allies abroad, but lead by example, underlining that disinformation knows no political party and that the United States is committed to reversing its normalization in our own political discourse.**

Once again, Chairman Langevin, Ranking Member Stefanik, and Members of the Subcommittee, it has been an honor to share my thoughts with you today, and I look forward to answering your questions.

---

[24] National Security Commission on Artificial Intelligence, 278.
[25] Global Affairs Canada, "Rapid Response Mechanism Canada - Protecting Democracy," GAC, June 9, 2019.

Nina Jankowicz

Nina Jankowicz studies the intersection of democracy and technology in Central and Eastern Europe. She is the author of How To Lose the Information War: Russia, Fake News, and the Future of Conflict (Bloomsbury/IBTauris). Ms. Jankowicz has advised the Ukrainian government on strategic communications under the auspices of a Fulbright- Clinton Public Policy Fellowship. Her writing has been published by The New York Times, The Washington Post, The Atlantic, and others. She is a frequent television and radio commentator on disinformation and Russian and Eastern European affairs. Prior to her Fulbright grant in Ukraine, Ms. Jankowicz managed democracy assistance programs to Russia and Belarus at the National Democratic Institute for International Affairs. She received her MA in Russian, Eurasian, and East European Studies from Georgetown University's School of Foreign Service.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the House of Representatives for the 117th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), and contracts or grants (including subcontracts and subgrants), or payments originating with a foreign government, received during the past 36 months either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. Rule 11, clause 2(g)(5) also requires nongovernmental witnesses to disclose whether they are a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing. As a matter of committee policy, the House Committee on Armed Services further requires nongovernmental witnesses to disclose the amount and source of any contracts or grants (including subcontracts and subgrants), or payments originating with any organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months either by the witness or by an entity represented by the witness. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number), will be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary. Please complete this form electronically.

Hearing Date: April 30, 2021

Hearing Subject:

"Technology and Information Warfare: The Competition for Influence and the Department of Defense"

Witness name: Nina Jankowicz

Position/Title: Disinformation Fellow, Wilson Center

Capacity in which appearing: (check one)

☑ Individual ☑ Representative

If appearing in a representative capacity, name of the organization or entity represented:

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
Grant	Smithsonian/Wilson Ctr	$30,000	Gender & disinfo research
Grant	US Embassy Norway	$100	Disinformation Event
Grant	US Embassy Brazil	$400	Disinformation/harassment event
Grant	US Embassy Spain	$400	Disinformation events

2020

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
Grant	Smithsonian/Wilson Ctr	$20,000	Disinformation research
Grant	US Embassy Norway	$200	Disinformation event

2019

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
Contract	NED/NDI	$3000	Lithuanian Disinformation Research
Grant	US Embassy Austria	$2792	Disinformation events

2018

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

Foreign Government Contract, Grant, or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants), or payments originating from a foreign government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
Contract	UK, via Zinc Network	$1313	Counter Disinformation advisory board
Contract	UK / Centre for Information Resilience	$2778	Counter Disinformation consulting/research
Contract	UK, via Sayara Int'l	$7,610	Gender & Disinfo Research/consulting

2020

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
Contract	UK, via Zinc Network	$1785	Counter Disinformation advisory board
Contract	UK, via Sayara Int'l	$1187	Counter Disinformation Consulting

2019

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
Payment	Canadian Defense Dept	$2577	Disinformation and elections consultations

2018

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

Fiduciary Relationships: If you are a fiduciary of any organization or entity that has an interest in the subject matter of the hearing, please provide the following information:

Organization or entity	Brief description of the fiduciary relationship

Organization or Entity Contract, Grant or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants) or payments originating from an organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months, please provide the following information:

2021

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment

2020

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Grant	Facebook via Wilson Center	$60,000	Disinformation Research

2019

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Grant	Facebook via Wilson Center	$30,000	Disinformation research

2018

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment

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.

Herbert Lin
Senior Research Scholar at the Center for International Security and Cooperation
Hank J. Holland Fellow in Cyber Policy and Security, Hoover Institution

Dr. Herb Lin is senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University. His research interests relate broadly to policy-related dimensions of cybersecurity and cyberspace, and he is particularly interested in the use of offensive operations in cyberspace as instruments of national policy and in the security dimensions of information warfare and influence operations on national security. In addition to his positions at Stanford University, he is Chief Scientist, Emeritus for the Computer Science and Telecommunications Board, National Research Council (NRC) of the National Academies, where he served from 1990 through 2014 as study director of major projects on public policy and information technology, and Adjunct Senior Research Scholar and Senior Fellow in Cybersecurity (not in residence) at the Saltzman Institute for War and Peace Studies in the School for International and Public Affairs at Columbia University; and a member of the Science and Security Board of the Bulletin of Atomic Scientists. In 2016, he served on President Obama's Commission on Enhancing National Cybersecurity. Prior to his NRC service, he was a professional staff member and staff scientist for the House Armed Services Committee (1986-1990), where his portfolio included defense policy and arms control issues. He received his doctorate in physics from MIT.

Avocationally, he is a longtime folk and swing dancer and a lousy magician. Apart from his work on cyberspace and cybersecurity, he is published in cognitive science, science education, biophysics, and arms control and defense policy. He also consults on K-12 math and science education.

DISCLOSURE FORM FOR WITNESSES
COMMITTEE ON ARMED SERVICES
U.S. HOUSE OF REPRESENTATIVES

INSTRUCTION TO WITNESSES: Rule 11, clause 2(g)(5), of the Rules of the House of Representatives for the 117th Congress requires nongovernmental witnesses appearing before House committees to include in their written statements a curriculum vitae and a disclosure of the amount and source of any federal contracts or grants (including subcontracts and subgrants), and contracts or grants (including subcontracts and subgrants), or payments originating with a foreign government, received during the past 36 months either by the witness or by an entity represented by the witness and related to the subject matter of the hearing. Rule 11, clause 2(g)(5) also requires nongovernmental witnesses to disclose whether they are a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing. As a matter of committee policy, the House Committee on Armed Services further requires nongovernmental witnesses to disclose the amount and source of any contracts or grants (including subcontracts and subgrants), or payments originating with any organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months either by the witness or by an entity represented by the witness. Please note that a copy of these statements, with appropriate redactions to protect the witness's personal privacy (including home address and phone number), will be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness's appearance before the committee. Witnesses may list additional grants, contracts, or payments on additional sheets, if necessary. Please complete this form electronically.

Hearing Date: April 30, 2021

Hearing Subject:

Technology and Information Warfare: The Competition for Influence and the Department of Defense

Witness name: Dr. Herbert Lin

Position/Title: Senior Research Scholar, Hank Holland Fellow, Stanford University

Capacity in which appearing: (check one)

● Individual ○ Representative

If appearing in a representative capacity, name of the organization or entity represented:

Federal Contract or Grant Information: If you or the entity you represent before the Committee on Armed Services has contracts (including subcontracts) or grants (including subgrants) with the federal government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant
none for any year listed			

2020

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2019

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

2018

Federal grant/ contract	Federal agency	Dollar value	Subject of contract or grant

Foreign Government Contract, Grant, or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants), or payments originating from a foreign government, received during the past 36 months and related to the subject matter of the hearing, please provide the following information:

2021

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment
none for any year listed			

2020

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2019

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

2018

Foreign contract/ payment	Foreign government	Dollar value	Subject of contract, grant, or payment

Fiduciary Relationships: If you are a fiduciary of any organization or entity that has an interest in the subject matter of the hearing, please provide the following information:

Organization or entity	Brief description of the fiduciary relationship
none	

Organization or Entity Contract, Grant or Payment Information: If you or the entity you represent before the Committee on Armed Services has contracts or grants (including subcontracts or subgrants) or payments originating from an organization or entity, whether public or private, that has a material interest in the subject matter of the hearing, received during the past 36 months, please provide the following information:

2021

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
none			

2020

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
none			

2019

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment
Honorarium	Lawrence Livermore National Lab	$5,000	for paper on special operations and information warfare

2018

Contract/grant/ payment	Entity	Dollar value	Subject of contract, grant, or payment

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Cyber, Innovative Technologies, and Information Systems, Committee on Armed Services, House of Representatives

For Release on Delivery
Expected at 3:00 p.m. ET
Friday, April 30, 2021

INFORMATION ENVIRONMENT

DOD Operations Need Enhanced Leadership and Integration of Capabilities

Statement of Joseph W. Kirschbaum, PhD,
Director, Defense Capabilities and Management

GAO@100

A Century of Non-Partisan Fact-Based Work

GAO-21-525T

GAO@100 Highlights

Highlights of GAO-21-525T, a testimony before the Subcommittee on Cyber, Innovative Technologies, and Information Systems, Committee on Armed Services, House of Representatives

Why GAO Did This Study

U.S. potential adversaries—including near-peer competitors Russia and China—are using information to achieve objectives below the threshold of armed conflict. DOD can use information operations to counter these activities.

This testimony summarizes GAO's past work related to DOD's IO capabilities. Specifically, it discusses: (1) DOD's information operation terms and concept, and (2) DOD's actions to implement the 2016 DOD IO strategy and address oversight and integration challenges. This statement is based on GAO's August and October 2019 reports (GAO-19-510C and GAO-20-51SU) and updates conducted in April 2021.

What GAO Recommends

In prior work on which this testimony is based, GAO recommended that DOD take five actions to improve leadership and integration for information operations—including that the department should conduct a posture review to assess integration challenges. DOD disagreed with the recommendations. However, Section 1631 of the National Defense Authorization Act for Fiscal Year 2020 included several provisions related to our recommendations, such as one that required the Secretary of Defense to conduct a posture review.

View GAO-21-525T. For more information, contact Joseph W. Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov.

April 30, 2021

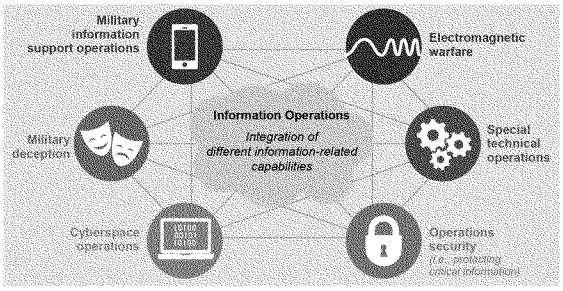
INFORMATION ENVIRONMENT

DOD Operations Need Enhanced Leadership and Integration of Capabilities

What GAO Found

At its core, information operations (IO) are the *integration* of information-related capabilities during military operations to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own. (See figure.) For example, in seeking to facilitate safe and orderly humanitarian assistance, the Department of Defense (DOD) would conduct IO by influencing host nation and regional cooperation through the *integration* of public affairs activities and military information support operations.

Figure: Information Operations and Selected Information-Related Capabilities



Source: GAO analysis of Department of Defense (DOD) information. | GAO 21-525T

GAO found, in 2019, that DOD had made limited progress in implementing the 2016 DOD IO strategy and faced a number of challenges in overseeing the IO enterprise and integrating its IO capabilities. Specifically:

- In seeking to implement the strategy, DOD had not developed an implementation plan or an investment framework to identify planning priorities to address IO gaps.
- DOD has established department-wide IO roles and responsibilities and assigned most oversight responsibilities to the Under Secretary of Defense for Policy. The Under Secretary had exercised some responsibilities, such as establishing an executive steering group. However, the Under Secretary had not fulfilled other IO oversight responsibilities, such as conducting an assessment of needed tasks, workload, and resources. Instead, the Under Secretary delegated these responsibilities to an official whose primary responsibilities are focused on special operations and combatting terrorism.
- DOD had integrated information-related capabilities in some military operations, but had not conducted a posture review to assess IO challenges. Conducting a comprehensive posture review to fully assess challenges would assist DOD in effectively operating while using information-related capabilities.

Chairman Langevin, Ranking Member Stefanik, and Members of the Subcommittee:

I am pleased to be here today to discuss the vital role of the Department of Defense's (DOD) operations in the information environment. In short, information environment refers to the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

As then Secretary of Defense Carter stated in the 2016 DOD *Strategy for Operations in the Information Environment,* although the term information environment is relatively new, the concept of an "information battlefield" is not. The role of information, either provided or denied, is an important consideration in military planning and operations. In fact, throughout the history of warfare, militaries have sought advantage through actions intended to affect the perception and behavior of adversaries. Information is such a powerful tool, it is recognized as an element of U.S. national power and, as such, the department must be prepared to synchronize information programs, plans, messages, and products as part of a whole-of-government effort.[1]

We are not the only global power to recognize the importance of the information environment. Competitors, including Russia and China, have made great strides in improving their capabilities and in how they use the information environment to advance their national objectives and to undermine the security and principles of the United States and its allies and partners. For example, Russia, through military intelligence units, also known as the "GRU," and Kremlin-linked troll organizations often referred to as the "Internet Research Agency," deploys information warfare operations against the United States and its allies and partners, with the goal of advancing the strategic interests of the Russian Federation.[2] Similarly, China has formed new military units to achieve dominance in the electromagnetic spectrum and centralized space, cyber, electromagnetic warfare capabilities, and potentially psychological

[1]DOD, *Strategy for Operations in the Information Environment* (June 2016).

[2]National Intelligence Council, *Foreign Threats to the 2020 US Federal Elections,* ICA 2020-00078D (Mar. 10, 2021).

warfare, according to studies we reviewed for our December 2020 report focused on DOD electromagnetic spectrum operations.[3]

As recognized in DOD's 2018 *Joint Concept for Operating in the Information Environment,* information technology has significantly enhanced human interaction around the globe and elevated the importance of information as an instrument of power wielded by individuals and societies in politics, economics, and warfare. Advances in information technology have significantly changed the generation of, transmission of, reception of, and reaction to information. These advances have increased the speed and range of information, diffused power over information, and shifted socio-cultural norms. However, our competitors and adversaries are taking advantage of the advances in information technology and subsequent effects in the information environment to offset the United States' preeminent warfighting force.

To make additional advances in this area, DOD has taken a number of actions—including issuing new or updated doctrine, establishing new leadership positions and organizations, and conducting operations. For example, in November 2012, DOD issued joint doctrine on Information Operations (IO).[4] Also, as noted earlier, DOD in 2016 issued its *Strategy for Operations in the Information Environment.* Additionally, in 2017, DOD updated its *Doctrine for the Armed Forces of the United States* to establish information as the seventh joint function of the military, along with the joint functions of command and control, intelligence, fires, movement and maneuver, protection, and sustainment.[5]

Finally, Congress addressed DOD's role in the information environment with a number of provisions in National Defense Authorization Acts—including requirements that led to DOD issuing the 2016 DOD *Strategy for Operations in the Information Environment,* the establishment of a

[3]GAO, *Electromagnetic Spectrum Operations: DOD Needs to Address Governance and Oversight Issues to Help Ensure Superiority*, GAO-21-64 (Washington, D.C.: Dec. 10, 2020).

[4]Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations* (Nov. 27, 2012, incorporating Change 1, Nov. 20, 2014).

[5]Joint Chiefs of Staff, Joint Publication 1, *Doctrine for the Armed Forces of the United States* (Mar. 25, 2013, incorporating Change 1, July 12, 2017).

DOD Principal Information Operations Advisor, and an IO posture review that the department has recently initiated.[6]

Since 2019, we have issued a series of reports assessing DOD operations in the information environment—including DOD cyberspace operations, information operations, and electromagnetic spectrum operations.[7] We have also issued reports on emerging threats to national security, threats attributed to emerging technology in the information environment (including 5G and internet-of-things devices), and units that conduct operations in the information environment.[8]

My testimony today describes (1) DOD's information operations terms and concept, and (2) DOD actions to implement the 2016 DOD strategy and address IO oversight and integration challenges.

This statement is based on our assessment of DOD documents that define and explain IO—including DOD's dictionary of military terms, DOD's IO policy directive, DOD's IO joint doctrine, and the 2016 DOD *Strategy for Operations in the Information Environment.*[9] This statement

[6]See, for example, Pub. L. No. 113-66, § 1096 (2013); and Pub. L. No. 116-92, § 1631 (2019).

[7]GAO, *Cyberspace Operations: DOD Has Authorities and Organizations in Place, but Policies, Processes, and Reporting Could Be Improved*, GAO-20-13C (Washington, D.C.: Sept. 28, 2020); GAO, *Information Operations: DOD Should Improve Leadership and Integration Efforts*, GAO-20-51SU (Washington, D.C.: Oct. 18, 2019); GAO-21-64; and GAO, *Electromagnetic Spectrum Operations: DOD Needs to Take Action to Help Ensure Superiority*, GAO-21-440T (Washington, D.C.: Mar. 19, 2021).

[8]GAO, *National Security: Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies*, GAO-19-204SP (Washington, D.C.: Dec. 13, 2018); *National Security: Actions Needed to Address 5G Telecommunications Risks*, GAO-21-256SU (Washington, D.C.: Mar. 5, 2021); *Internet of Things: Information on Use by Federal Agencies*, GAO-20-577 (Washington, D.C.: Aug. 13, 2020); and *Future Warfare: Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations*, GAO-19-570 (Washington, D.C.: Aug. 15, 2019).

[9]Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (as of January 2021); DOD, DOD Directive 3600.01, *Information Operations* (IO) (May 2, 2013, Incorporating Change 1, May 4, 2017); Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations* (Nov. 27, 2012, incorporating Change 1, Nov. 20, 2014); and DOD, *Strategy for Operations in the Information Environment.*

is also based on reports we issued in August and October 2019.[10] In addition, we obtained updates in April 2021. To conduct that work, we compared DOD strategy and guidance documents to actions taken by the department to determine the extent to which they had been implemented, interviewed DOD officials, and reviewed guidance documents regarding DOD oversight and integration of IO by selected DOD components. Our 2019 reports provide more details on the scope of our prior work and methodologies we used.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions, based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

IO-Related Terms and Examples of the IO Concept

Definitions for IO-Related Terms

DOD and others, including the Congressional Research Service and RAND, have IO-related terms as shown in figure 1.

[10]The report issued in August 2019 is a classified report. The report issued in October 2019 is a For Official Use Only version of the classified report. Both reports addressed the same objectives and use the same methodology. GAO, *Information Operations: DOD Should Improve Leadership and Integration Efforts*, GAO-19-510C (Washington, D.C.: Aug. 28, 2019) (S//NF); and GAO-20-51SU.

Figure 1: Information Operations-Related Terms Defined by DOD and Others

DOD-defined terms	Information environment	The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions, which continuously interact with individuals, organizations, and systems. These dimensions are known as the physical, informational, and cognitive (or human) dimensions.
	Information operations	The integrated employment during military operations of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.
	Information-related capability	A tool, technique, or activity employed within a dimension of the information environment that can be used to achieve a specific end. DOD does not have a definitive list of information-related capabilities because any capability could be used in a way that meets the definition, according to DOD officials. A DOD official recently told us that the term information-related capability will be retired from the common vocabulary, but for the purpose of this testimony the term will continue to be used.
Non-DOD-defined terms	Influence activities/ operations	DOD's current dictionary does not refer to the term "influence activities" or "influence operations." However, DOD's IO policy document refers to "influence activities" as an information-related capability, although the policy document does not define or describe these activities.[a] In 2009, RAND issued a study on behalf of the U.S. Army. In that study, RAND defines influence operations as "the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster attitudes, behaviors, or decisions by foreign target audiences that further U.S. interests and objectives."[b] A key difference between this definition of influence operations and DOD's definition of "information operations" is that RAND's definition includes all instruments of national power (i.e., diplomacy, information, military, and economics) whereas DOD's joint doctrine focuses on activities and operations conducted by the military.
	Information warfare	Neither the U.S. government (as a whole) nor DOD (as a department) have a definition for "information warfare." However, the Congressional Research Service notes that information warfare is a form of political warfare where targets include a nation state's government, military, private sector, and general population.[c] Taking place below the level of armed conflict, information warfare is the range of military and government operations to protect and exploit the information environment. It consists of both offensive and defensive operations: the protection and assurance of one's own information (information security), and information operations to advance interests. As noted in our 2019 report about DOD information operations, while DOD does not have a department-wide definition for information warfare, we found that several of the services were using the term.[d] For example, the U.S. Navy defines information warfare as the integrated application of capabilities to degrade, deny, deceive, or destroy an enemy's information environment or to enhance the effectiveness of friendly operations. Our report also noted that the U.S. Army has begun to use the term information warfare as well, but this change has not been made in doctrine or guidance.

Source: GAO analysis of Congressional Research Service, Department of Defense (DOD), and RAND information. | GAO-21-525T

[a]DOD DOD Dictionary of Military and Associated Terms, (As of January 2021); and DOD Directive 3600.01, Information Operations (IO), (May 2, 2013, Incorporating Change 1, May 4, 2017).

[b]RAND, Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities (2009).

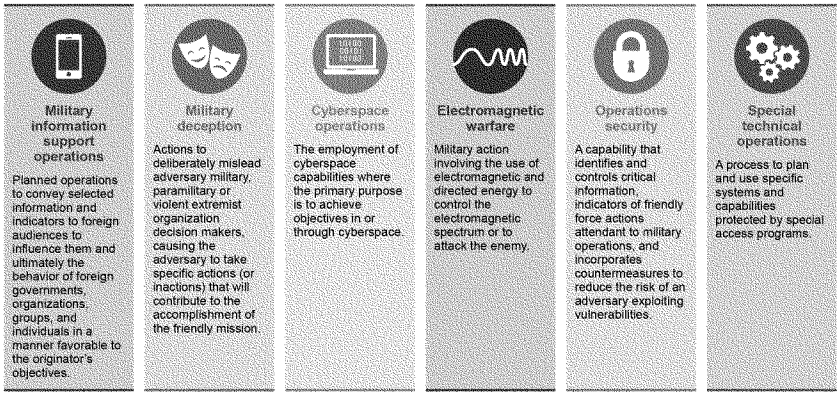
[c]Congressional Research Service, Information Warfare: Issues for Congress, R45142 (updated Mar. 5, 2018).

[d]GAO, Information Operations: DOD Should Improve Leadership and Integration Efforts, GAO-20-51SU (Washington, D.C.: Oct. 18, 2019).

DOD can employ different information-related capabilities to achieve the commander's goals. To take advantage of the benefits of different capabilities and achieve greater effects, commanders can develop plans and execute operations that use two or more capabilities. Figure 2

highlights selected information-related capabilities that are identified in the 2016 DOD *Strategy for Operations in the Information Environment.* Others may include public affairs, civil-military operations, intelligence capabilities, and key-leader engagement.[11]

Figure 2: Examples of DOD Information-Related Capabilities



Source: GAO analysis of Department of Defense (DOD) information. | GAO-21-525T

Although DOD has defined information environment, information operations, and information-related capabilities, DOD officials have acknowledged that DOD has had challenges agreeing to a common set of terms or definitions. For example, while neither DOD's dictionary of terms, IO policy directive, nor IO joint doctrine uses the term "Information Warfare," we previously reported that the Navy and Army are using this term.[12] We have also found that DOD does not have a complete list of

[11]DOD Directive 3600.01, *Information Operations (IO)*, also identifies "influence activities" as an example of information-related capabilities. However, the directive does not define the term or identify the type of activities that would be considered "influence activities."

[12]*DOD Dictionary of Military and Associated Terms*, DOD Directive 3600.01, Joint Publication 3-13, and GAO-20-51SU.

information-related capabilities because, according to DOD officials, any capability could be used in a way that meets the current definition. Consequently, it could be challenging for combatant commanders to utilize IO as the principal mechanism to integrate, synchronize, employ, and adapt all information-related capabilities in the information environment to accomplish operational objectives against adversaries and potential adversaries, as required by DOD's IO policy directive.[13] DOD IO officials told us they have been working with DOD components to develop a more consistent set of IO-related terms while updating the IO strategy and joint doctrine.

Examples of Information Operations

DOD doctrine on IO describes how information-related capabilities can be used to create lethal and nonlethal effects to support achievement of the objectives to reach the desired end state. As highlighted in the following examples, DOD IO planners can *integrate* more than one information-related capability to achieve the commander's desired end-state and it is this integration that enables desired effects in and through the information environment at specified times and locations.[14]

- DOD's joint doctrine on IO presents a hypothetical example where an adversary attempts to overthrow a country's government using lethal and nonlethal means to demonstrate that the government is not fit to support and protect its people.[15] To counter the adversary, DOD—working with other U.S. government agencies and the country's government and institutions—could mitigate the adversary's effectiveness through integrated planning and execution of information-related capabilities such as military information support operations, military deception, electromagnetic operations, cyberspace operations, security force assistance, combat operations, key leader engagement, and public affairs.
- The Air Force's IO doctrine highlighted that a commander could employ IO during a humanitarian assistance operation. The commander could influence host nation and regional cooperation and facilitate safe and orderly humanitarian assistance through the

[13]DOD Directive 3600.01

[14]*DOD Strategy for Operations in the Information Environment* (June 2016).

[15]Joint Publication 3-13.

integration of public affairs activities and military information support operations messaging.[16]

DOD Has Made Limited Progress Implementing Its 2016 Strategy and Addressing IO Oversight and Integration Challenges

DOD Has Made Limited Progress Implementing Its 2016 IO Strategy

DOD's 2016 Strategy for Operations in the Information Environment was intended to "signal [the department's] commitment and resolve" and provide the Secretary of Defense's guidance on important steps that DOD must take as a department to enhance its ability to conduct military operations. Our 2019 report highlighted several actions that DOD took in response to its *2016 Strategy for Operations in the Information Environment.* For example:

- In March 2018, DOD issued the *Joint Concept for Integrated Campaigning* which addresses DOD's role in achieving U.S. goals outside of the traditional military sphere—such as competition below the threshold of armed conflict.[17]
- In July 2018, DOD issued the *Joint Concept for Operating in the Information Environment* to institutionalize and operationalize the military's approach to information operations so that the department can better compete with state and non-state actors.[18] The document describes how DOD can use information to influence others' behavior. For example, the concept states that DOD and its allies must be able to communicate a compelling narrative and anticipate and proactively counter an adversary's attempt to manipulate information.

[16]Air Force, Air Force Doctrine Publication 3-13, *Information Operations* (Apr. 28, 2016).

[17]Joint Chiefs of Staff, *Joint Concept for Integrated Campaigning* (Mar. 16, 2018).

[18]Joint Chiefs of Staff, *Joint Concept for Operating in the Information Environment (JCOIE)* (July 25, 2018).

However, as we reported in October 2019, DOD had not fully implemented its strategy. For example, DOD did not issue an implementation plan or an investment framework to guide the implementation of the strategy. OSD officials told us that the department was unable to fully implement the 2016 *Strategy for Operations in the Environment* because many of the tasks the department included in the strategy were not written in a way the department could execute. We reported that this may be the case with some tasks, but we determined that the primary cause of the uneven progress was in part due to the IO Executive Steering Group not implementing a process to facilitate and oversee the execution of the 2016 strategy. For example, the IO Executive Steering Group had not developed:

- an implementation plan and quarterly (or more frequent) progress reviews on the status of the strategy's implementation; and
- an investment framework that would identify planning priorities to address IO gaps.

Instead, during this timeframe, the IO Executive Steering Group shifted its focus and developed the *Joint Concept of Operations in the Information Environment,* conducted a capabilities-based assessment of DOD's ability to operate in the information environment, and then started developing a new IO strategy.

We recommended that DOD establish a process that facilitates implementation of DOD's revised strategy for operations in the information environment and hold DOD components accountable for implementing this strategy. DOD did not concur with this recommendation.[19]

In April 2021, a DOD official told us that the department is updating the 2016 DOD *Strategy for Operations in the Information Environment* while it completes an analysis of capability gaps for operations in the information environment (i.e., posture review) that we had also recommended and Congress subsequently mandated the department complete.[20] According to the officials, once the Secretary of Defense issues the updated

[19]In our 2019 report, DOD deemed its response to this recommendation as sensitive information not subject to public release. As a result, we are unable to elaborate on DOD's response.

[20]GAO-20-51SU and Pub. L. No. 116-92, § 1631 (2019).

strategy, the Principal IO Advisor will use a process to oversee implementation of the IO strategy similar to one used by the DOD Principal Cyber Advisor to oversee the implementation of the DOD Cyber Strategy.[21]

DOD Has Established Roles and Responsibilities for IO, but Has Oversight and Integration Challenges

DOD Roles and Responsibilities

In our 2019 report, we highlighted that DOD had established department-wide IO roles and responsibilities and assigned many of them to the Under Secretary of Defense for Policy (USD (Policy)). The Under Secretary has exercised some of those responsibilities, such as establishing the IO Executive Steering Group. However, the Under Secretary had not fulfilled other IO oversight responsibilities. Figure 3 shows the roles and responsibilities for IO established by DOD.

[21]The DOD Principal Cyber Advisor established multiple oversight processes in support of the 2015 DOD Cyber Strategy, according to officials from the Office of the DOD Principal Cyber Advisor. These oversight processes included (1) the issuance of an overall implementation plan (or individual plans for different sections of the strategy) that identifies specific actions that will be taken and estimated completion dates, (2) assignment of senior DOD leader(s) (e.g., general and flag officers and/or civilian senior executives) who would be held accountable for implementing a specific section of the strategy, and (3) establishing progress reports (e.g., monthly, bimonthly, or quarterly) on the status of the actions identified in the implementation plan(s). The DOD Principal Cyber Advisor was able to use these oversight processes to monitor DOD's progress for the 2015 and 2018 cyber strategies.

Figure 3: DOD Roles and Responsibilities for Information Operations

Under Secretary of Defense for Policy	**Principal Staff Advisor to the Secretary of Defense** In this role, the Under Secretary of Defense for Policy is the principal staff advisor to the Secretary of Defense and responsible for information operations (IO) oversight and management. **Senior DOD IO Official** In response to a requirement in the National Defense Authorization Act for Fiscal Year 2018, the Deputy Secretary of Defense designated the Under Secretary of Defense for Policy as the senior official for overseeing the integration of strategic IO and cyber-enabled IO. According to the memorandum, this designation was consistent with the Under Secretary's existing roles and responsibilities for IO.[a] However, as noted below the Under Secretary of Defense for Policy has largely delegated responsibilities associated with principal staff advisor and senior DOD IO official to the Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism, according to Office of the Secretary of Defense officials. **Co-Chair, IO Executive Steering Group** Co-chairs the primary coordination forum within DOD to inform, coordinate, and resolve IO issues among the DOD components. The Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism fulfills this role. **Principal Information Operations Advisor[b]** Responsible for the overall integration and supervision of the deterrence of, conduct of, and defense against information operations and promulgation of policies to ensure adequate coordination and deconfliction with the Department of State, the intelligence community, and other federal agencies, among other things.
IO Cross Functional Team	Consistent with Section 1631 of the National Defense Authorization Act for Fiscal Year 2020, DOD is in the process of establishing a full-time cross functional team composed of subject-matter experts selected from organizations within the Office of the Secretary of Defense, Joint Staff, military departments, defense agencies, and combatant commands, according to DOD officials.[c]
IO Executive Steering Group	**DOD's Senior Deliberative and Advisory Board for IO** Responsible for implementing the 2016 *DOD Strategy for Operations in the Information Environment* and providing input and recommendations to select Office of Secretary of Defense and Joint Staff processes.
DASD for Special Operations and Combating Terrorism	**Principal Staff Advisor to the Secretary of Defense (*delegated*), Senior DOD IO Official, and Co-Chair of the IO Executive Steering Group** According to Office of the Secretary of Defense officials, the Under Secretary of Defense for Policy has largely delegated responsibilities for these roles to this official. Also, responsible for DOD policy related to special operations forces and personnel recovery, among other things.
Chairman of the Joint Chiefs of Staff	**Joint IO Proponent** The responsibilities of the Joint IO Proponent include three areas: joint policy and doctrine; planning, operations, and assessment; and force development.
Joint Staff Deputy Director for Global Operations	**Joint IO Proponent (*delegated*)** Executes the Joint IO Proponent responsibilities on the chairman's behalf. These day-to-day responsibilities include acting as co-chair of the IO Executive Steering Group and overseeing IO policy execution within the combatant commands and joint task forces.
Joint Information Operations Warfare Center	Assists the Joint IO Proponent (J39) in the execution of responsibilities and provides direct support to combatant commanders to include planning guidance. Also, provides IO support to analysis, planning and assessment of chairman plans and orders.
Military services[d]	The military services organize, train, equip, and provide forces for military operations, including IO and information-related capabilities. All military services have undertaken organizational steps to better position themselves for IO and to provide IO personnel to support combatant commands' military operations.
Combatant Commands	Utilizes IO as the principal mechanism to integrate, synchronize, employ, and adapt all information-related capabilities in the information environment to accomplish operational objectives against adversaries and potential adversaries. Develops, plans, programs and assesses IO as well as information-related capabilities execution in support of IO during all phases of military engagement and at all levels of war.

DASD Deputy Assistant Secretary of Defense

Source: GAO analysis of Department of Defense (DOD) information. | GAO-21-525T

[a]Deputy Secretary of Defense Memorandum, Designated Senior Official for the Integration of Strategic Information Operations and Cyber-Enabled Information Operations (June 13, 2018) and Pub. L. No. 115-91, § 1637 (2017). The statute requires the designated senior official to implement and oversee processes and procedures related to information operations.

[b]DOD is in the process of pursuing a full-time, Deputy Principal Information Operations Advisor, according to DOD officials. The Deputy will be a general or flag officer who oversees the Information Operations Cross-Functional Team and report directly to USD (Policy).

[c]Pub. L. No. 116-92, § 1631 (2019).

[d]For the purposes of our 2019 report, we referred to the military services as including the Army, Marine Corps, Navy, and Air Force. The Coast Guard and Space Force, although both military services, were not included in the scope of our review.

Oversight Challenges

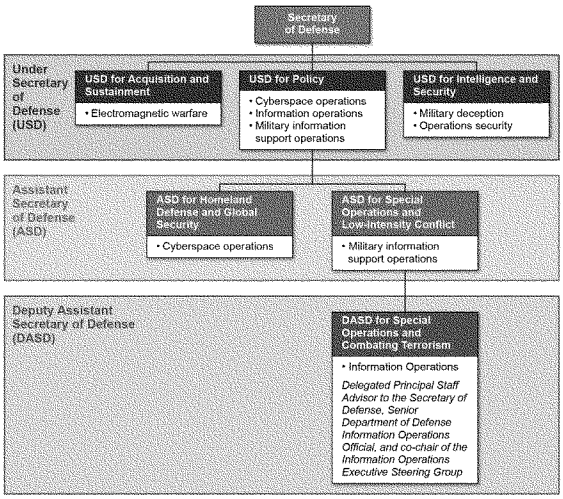
DOD has established department-wide IO roles and responsibilities and, as noted above, assigned most to the USD (Policy). The Under Secretary has exercised some responsibilities, such as establishing an executive steering group. However, the Under Secretary had not fulfilled other IO oversight responsibilities.[22]

One of the challenges in managing and overseeing IO efforts is that the majority of IO responsibilities have been delegated to a Deputy Assistant Secretary of Defense (and whose primary focus is on special operations and combatting terrorism), according to DOD officials. As shown in figure 4, there are different leaders within the Office of the Secretary of Defense who are responsible for individual information-related capabilities and all of them outrank the Deputy Assistant Secretary of Defense, report to a different Under Secretary of Defense, or both.[23]

[22]In our 2019 report, DOD deemed specific examples of how the department had not implemented the strategy as sensitive information not subject to public release. As such, this written statement is unable to elaborate on specific actions not taken.

[23]Conversely, according to the Acting Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, "Russia sees the information domain differently than the United States and its allies and partners and that Russian publications and actions indicate its government maintains a holistic concept of 'information confrontations'." Similarly, a 2018 National Defense University paper about China's Strategic Support Force states the Strategic Support Force combines assorted space, cyber, electromagnetic, and psychological warfare capabilities from across the People's Liberation Army services and its former General Department. DOD, Joint Statement for the Record of Mr. Christopher Maier, Acting Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, Mr. Neill Tipton, Director of Defense Intelligence (Collections and Special Programs), and Mr. James Sullivan, Defense Intelligence Officer for Cyber, Defense Intelligence Agency before House Armed Services Committee Subcommittee on Intelligence and Special Operations on "Disinformation in the Gray Zone: Opportunities, Limitations, Challenges." (Mar. 16. 2021). National Defense University, China's Strategic Support Force: A Force for a New Era (Washington, D.C.: December 2018).

Figure 4: Responsibilities for Some Information-Related Capabilities across the Office of the Secretary of Defense



Source: GAO analysis of Office of the Secretary of Defense information. | GAO-21-525T

During our 2019 review, we found two underlying factors on why the USD (Policy) had not fulfilled required oversight responsibilities for managing IO across DOD.

First, we found that the USD (Policy) had not assessed the tasks, workload, or the resources needed to manage, oversee, and coordinate IO in the department, including the activities of the other offices responsible for specific information-related capabilities. In 2018, the Deputy Secretary of Defense initially designated the USD (Policy) as the senior DOD IO official and directed an analysis of new tasks, potential

workload, and resource requirements of the designation.[24] However, we asked officials in the Office of the USD (Policy) about the analysis, and they said the office has not conducted such an assessment. We recommended that the USD (Policy) assess the new tasks, potential workload, and resources needed to fulfill required oversight responsibilities for managing IO across DOD and hold accountable the other offices overseeing the information-related capabilities. DOD did not concur with this recommendation.[25] However, in April 2021, a DOD official told us that the Secretary of Defense had approved additional resources to support IO leadership efforts.

Second, we found that DOD had not issued policy formalizing the IO Executive Steering Group's responsibilities for providing IO oversight and management and deconflicting and resolving issues within the department in accordance with DOD's IO directive. This has left the group without authority to exercise its oversight role, according to OSD officials. We recommended that the USD (Policy) issue policy identifying the IO Executive Steering Group's formal responsibilities for providing IO oversight and management and deconflicting and resolving issues within the department. DOD did not concur with this recommendation.[26] In April 2021, a DOD official told us that the IO Executive Steering Group will maintain its advisory role. Some of the issues we heard during our 2019 review may be mitigated by the new IO Cross-Functional Team that DOD subsequently established in response to a requirement in the National Defense Authorization Act for Fiscal Year 2020.[27]

Integration Challenges

In our 2019 report, we highlighted that DOD had integrated information-related capabilities in some military operations, but had not addressed key planning, coordination, and operational challenges. Specifically, DOD

[24]Deputy Secretary of Defense, *Designated Senior Official for the Integration of Strategic Information Operations and Cyber-Enabled Information Operations*.

[25]In our 2019 report, DOD deemed its response to this recommendation as sensitive information not subject to public release. As a result, we are unable to elaborate on DOD's response.

[26]In our 2019 report, DOD deemed its response to this recommendation as sensitive information not subject to public release. As a result, we are unable to elaborate on DOD's response.

[27]Pub. L. No. 116-92, § 1631 (2019). The IO Cross-Functional Team will report directly to a full-time Deputy Principal IO Advisor that DOD is in the process of selecting, according to DOD officials. The Deputy Principal IO Advisor will be a general officer or flag officer and report directly to the USD (Policy).

had not assessed these challenges or clearly defined roles and responsibilities between geographic combatant commands and U.S. Cyber Command. Consequently, we recommended that DOD conduct a comprehensive posture review to fully assess challenges. Such a posture review would assist DOD in more effectively operating while using information-related capabilities. We also recommended that DOD clearly define roles and responsibilities between geographic combatant commands and U.S. Cyber Command. Such action would enable DOD to more effectively plan and execute operations across boundaries and below the level of conflict. DOD did not concur with these recommendations.[28] However, the National Defense Authorization Act for Fiscal Year 2020 included a provision that required the Secretary of Defense to conduct such a posture review.[29] In April 2021, DOD officials told us that the department had taken initial steps for the posture review, but did not provide an estimated completion date. The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 places a limitation on funding until DOD completes this posture review and issues an updated IO strategy.[30]

In conclusion, it is important that DOD continues to take actions that recognize the value of information as a joint function and conduct operations in the information environment. The United States remains in competition with our potential adversaries in strengthening our respective capabilities in the information environment. DOD has made some progress, but there are opportunities for improved leadership and for integration of IO. It is important that our military continue efforts to put in place the necessary people, policies, programs, and partnerships to defend against these new threats in the information environment. I look forward to continuing to work with this committee and the department to help it address these challenges and make the most of these opportunities.

Chairman Langevin, Ranking Member Stefanik, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions you may have at this time.

[28]In our 2019 report, DOD deemed its response to these recommendations as sensitive information not subject to public release. As a result, we are unable to elaborate on DOD's response.

[29]Pub. L. No. 116-92, § 1631(g).

[30]Pub. L. No. 116-283, § 1749 (2021).

GAO Contact and Staff Acknowledgments

If you or your staff members have any questions about this testimony, please contact Joseph W. Kirschbaum, Director, Defense Capabilities and Management, at (202) 512-9971 or Kirschbaumj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Tommy Baril (Assistant Director), Neil Feldman (Analyst-in-Charge), Tracy Barnes, Mallory Bryan, Jeffrey Cirillo, Benjamin Emmel, Evan Keir, Amie Lesser, Ricardo A. Marquez, Richard Powelson, Breana Stevens, and Yee Wong. GAO staff who made key contributions to the 2019 report that part of this testimony is based on are Tommy Baril (Assistant Director), Jennifer Spence (Analyst-in-Charge), Tracy Barnes, Nicholas Benne, Christopher Gezon, Amie Lesser, Ned Malone, Richard Powelson, and Garrett Riba.

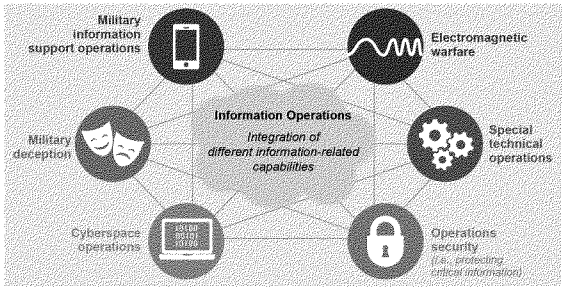
GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts. Visit GAO on the web at https://www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact FraudNet: Website: https://www.gao.gov/about/what-gao-does/fraudnet Automated answering system: (800) 424-5454 or (202) 512-7700
Congressional Relations	Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548
Strategic Planning and External Liaison	Stephen J. Sanford, Acting Managing Director, spel@gao.gov, (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548

Figure 1: Information Operations-Related Terms Defined by DOD and Others

DOD-defined terms	Information environment	The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions, which continuously interact with individuals, organizations, and systems. These dimensions are known as the physical, informational, and cognitive (or human) dimensions.
	Information operations	The integrated employment during military operations of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.
	Information-related capability	A tool, technique, or activity employed within a dimension of the information environment that can be used to achieve a specific end. DOD does not have a definitive list of information-related capabilities because any capability could be used in a way that meets the definition, according to DOD officials. GAO recently learned that the term information-related capability will be retired from the common vocabulary, but for the purpose of this testimony the term will continue to be used.
Non-DOD-defined terms	Influence activities/ operations	DOD's current dictionary does not refer to the term "influence activities" or "influence operations." However, DOD's IO policy document refers to "influence activities" as an information-related capability, although the policy document does not define or describe these activities.[a] In 2009, Rand issued a study on behalf of the U.S. Army. In that study, Rand defines influence operations as "the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster attitudes, behaviors, or decisions by foreign target audiences that further U.S. interests and objectives."[b] A key difference between this definition of influence operations and DOD's definition of "information operations" is that Rand's definition includes all instruments of national power (i.e., diplomacy, information, military, and economics) whereas DOD's joint doctrine focuses on activities and operations conducted by the military.
	Information warfare	Neither the U.S. government (as a whole) nor DOD (as a department) have a definition for "information warfare." However, the Congressional Research Service notes that information warfare is a form of political warfare where targets include a nation state's government, military, private sector, and general population.[c] Taking place below the level of armed conflict, information warfare is the range of military and government operations to protect and exploit the information environment. It consists of both offensive and defensive operations: the protection and assurance of one's own information (information security), and information operations to advance interests. As noted in our 2019 report about DOD information operations, while DOD does not have a department-wide definition for information warfare, we found that several of the services were using the term.[d] For example, the U.S. Navy defines information warfare as the integrated application of capabilities to degrade, deny, deceive, or destroy an enemy's information environment or to enhance the effectiveness of friendly operations. Our report also noted that the U.S. Army has begun to use the term information warfare as well, but this change has not been made in doctrine or guidance.

Source: GAO analysis of Congressional Research Service, Department of Defense (DOD), and RAND information. | GAO-21-525T

Figure: Information Operations and Selected Information-Related Capabilities



Source: GAO analysis of Department of Defense (DOD) information. | GAO 21-525T

Figure 2: Examples of DOD Information-Related Capabilities

Military information support operations
Planned operations to convey selected information and indicators to foreign audiences to influence them and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives.

Military deception
Actions to deliberately mislead adversary military, paramilitary or violent extremist organization decision makers, causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.

Cyberspace operations
The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

Electromagnetic warfare
Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.

Operations security
A capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities.

Special technical operations
A process to plan and use specific systems and capabilities protected by special access programs.

Source: GAO analysis of Department of Defense (DOD) information. | GAO 21-525T

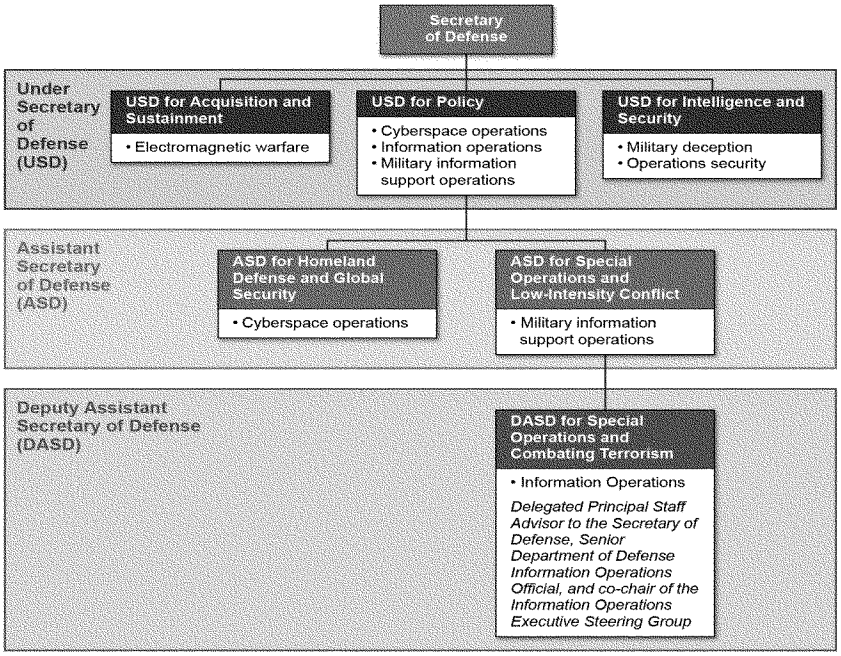
Figure 3: DOD Roles and Responsibilities for Information Operations

Under Secretary of Defense for Policy	**Principal Staff Advisor to the Secretary of Defense** In this role, the Under Secretary of Defense for Policy is the principal staff advisor to the Secretary of Defense and responsible for information operations (IO) oversight and management. **Senior DOD IO Official** In response to a requirement in the National Defense Authorization Act for Fiscal Year 2018, the Deputy Secretary of Defense designated the Under Secretary of Defense for Policy as the senior official for overseeing the integration of strategic IO and cyber-enabled IO. According to the memorandum, this designation was consistent with the Under Secretary's existing roles and responsibilities for IO.[a] However, as noted below the Under Secretary of Defense for Policy has largely delegated responsibilities associated with principal staff advisor and senior DOD IO official to the Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism, according to Office of the Secretary of Defense officials. **Co-Chair, IO Executive Steering Group** Co-chairs the primary coordination forum within DOD to inform, coordinate, and resolve IO issues among the DOD components. The Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism fulfills this role. **Principal Information Operations Advisor[b]** Responsible for the overall integration and supervision of the deterrence of, conduct of, and defense against information operations and promulgation of policies to ensure adequate coordination and deconfliction with the Department of State, the intelligence community, and other federal agencies, among other things.
IO Cross Functional Team	Consistent with Section 1631 of the National Defense Authorization Act for Fiscal Year 2020, DOD is in the process of establishing a full-time cross functional team composed of subject-matter experts selected from organizations within the Office of the Secretary of Defense, Joint Staff, military departments, defense agencies, and combatant commands, according to DOD officials.[c]
IO Executive Steering Group	**DOD's Senior Deliberative and Advisory Board for IO** Responsible for implementing the 2016 *DOD Strategy for Operations in the Information Environment* and providing input and recommendations to select Office of Secretary of Defense and Joint Staff processes.
DASD for Special Operations and Combating Terrorism	**Principal Staff Advisor to the Secretary of Defense (*delegated*), Senior DOD IO Official, and Co-Chair of the IO Executive Steering Group** According to Office of the Secretary of Defense officials, the Under Secretary of Defense for Policy has largely delegated responsibilities for these roles to this official. Also, responsible for DOD policy related to special operations forces and personnel recovery, among other things.
Chairman of the Joint Chiefs of Staff	**Joint IO Proponent** The responsibilities of the Joint IO Proponent include three areas: joint policy and doctrine; planning, operations, and assessment; and force development.
Joint Staff Deputy Director for Global Operations	**Joint IO Proponent (*delegated*)** Executes the Joint IO Proponent responsibilities on the chairman's behalf. These day-to-day responsibilities include acting as co-chair of the IO Executive Steering Group and overseeing IO policy execution within the combatant commands and joint task forces.
Joint Information Operations Warfare Center	Assists the Joint IO Proponent (J39) in the execution of responsibilities and provides direct support to combatant commanders to include planning guidance. Also, provides IO support to analysis, planning and assessment of chairman plans and orders.
Military services[d]	The military services organize, train, equip, and provide forces for military operations, including IO and information-related capabilities. All military services have undertaken organizational steps to better position themselves for IO and to provide IO personnel to support combatant commands' military operations.
Combatant Commands	Utilizes IO as the principal mechanism to integrate, synchronize, employ, and adapt all information-related capabilities in the information environment to accomplish operational objectives against adversaries and potential adversaries. Develops, plans, programs and assesses IO as well as information-related capabilities execution in support of IO during all phases of military engagement and at all levels of war.

DASD Deputy Assistant Secretary of Defense

Source: GAO analysis of Department of Defense (DOD) information. | GAO-21-525T

Figure 4: Responsibilities for Some Information-Related Capabilities across the Office of the Secretary of Defense



Source: GAO analysis of Office of the Secretary of Defense information. | GAO-21-525T

Joseph W. Kirschbaum, PhD

Joe Kirschbaum is a Director in the Defense Capabilities and Management Team of the U.S. Government Accountability Office (GAO). He assists congressional committees by overseeing evaluations of U.S. Government programs in the Strategic Warfare and Intelligence area, focusing mostly on the Department of Defense.

Over his 27-year career with GAO, Mr. Kirschbaum conducted and led audits throughout the range of defense and national security programs. Among the topics he has covered are U.S. strategic nuclear forces; military cyberspace doctrine and operations; information operations; intelligence, surveillance, and reconnaissance; counterproliferation of weapons of mass destruction; chemical, biological, radiological, nuclear, and high-yield explosive preparedness and consequence management; homeland defense; Army and Navy force structure; and development of the Navy's littoral combat ship. In 2013 Mr. Kirschbaum served as an acting director in GAO's Homeland Security and Justice Team, overseeing evaluations of federal emergency preparedness and homeland security programs.

Mr. Kirschbaum comes from a Navy family and upon graduating High School served briefly on active duty in the U.S. Navy's nuclear propulsion program. Mr. Kirschbaum has a Bachelors degree in History and Political Science, a Masters degree in National Security Studies (both from California State University, San Bernardino) and a Ph.D in military history from George Washington University.

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

APRIL 30, 2021

QUESTIONS SUBMITTED BY MR. MOULTON

Mr. MOULTON. I am disheartened by the dramatic drop in the public's trust and confidence in the U.S. military from 70% to 56% that you point out in your written testimony, Mr. Gerstell. Trust between the people and the military is vital to a democratic nation and to the health of an All-Volunteer Force. While this drop in confidence may be influenced by external disinformation, do you believe service members' own social media activity, personal or professional, may play a role in negatively impacting the public's views on the military? Are there policy recommendations you would make to the services to ensure the U.S. military retains the public's trust without impeding troops' freedom of speech?

Mr. GERSTELL. Thank you Representative Moulton for the opportunity to respond to your questions. I am not an expert on military matters so I will address this from the point of view of a former national security official who has studied online disinformation generally. As you know, a number of academicians, cyber researchers and think tanks have sought to determine the extent to which trust in societal institutions can be undermined—and thus democracy corroded—by disinformation and the corresponding expression of extremist views. Surveys indicate that reinforcing and amplifying factors play a key role in instilling and confirming hateful or erroneous beliefs in people exposed to extremist speech and false information. The identity of the communicators spreading the speech disinformation and corroboration and enhancement by opinion leaders are all factors in promoting the "effectiveness" of extremist speech and disinformation. It thus stands to reason that when the general public sees social media posts by members of the military espousing hateful or extremist positions that are aligned with what the public might be predisposed to accept based on prior exposure to disinformation from non-military sources, it inevitably combines to shape the public's view of the military. That type of reinforcing and corroborating action has a potent effect on influencing what people believe. In short, it's hard to believe that social media posts (positive and negative) by members of the military don't have any effect on the public's perception of our armed forces. As you note, it is of course vital that our military enjoys the strong approval and trust of the American public, for purposes of recruiting, assistance to veterans and obviously support in times when our troops are in harm's way. Social media activity by members of the military that do not reflect well on that institution can have an insidious and ultimately pernicious effect on this level of needed approval and trust. Countering problematic speech is difficult given how strongly our nation prizes freedom of speech, and it is sometimes hard to draw the line between improper hateful expressions that should be curtailed for the good of society, and merely distasteful if not repugnant opinions. But the mere fact that it's difficult to draw the line doesn't mean we should abandon any effort in this regard. Indeed, we have legal room to maneuver in this area; the law allows stricter regulation of the armed services than the general public, and the First Amendment is not absolute (to be clear, this is not to suggest any diminution of the latter's scope). Secretary Austin's standdown day was an important substantive as well as symbolic step, and clearly the military can do more with internal training and education. But many young men and women come to the military with little knowledge of how our government works or the underlying values upon which our democracy was founded, because of the almost total dearth of civic education in high school and lower grades. Fixing that problem alone would help minimize extremism in the military.

Mr. MOULTON. Mr. Gerstell, you have advocated for an integrated disinformation center within the Federal Government, aligning the many departments and agencies that have a role in information digital communications and creating a central node for responsibility over this issue. The NSCAI has made a similar recommendation. Can you describe in more detail what you envision this center to look like? What authorities or capabilities would this center need to be effective?

Mr. GERSTELL. Representative Moulton, the establishment of an integrated "disinformation" center, bring together all relevant parts of the federal government as well as the private sector, is one of the most crucial steps we can take in tackling the problem of disinformation.

While purely domestically generated disinformation is indeed a problem, it is made much worse by amplification and expansion by foreign adversaries that exploit the natural divisions in our society; and of course, those foreign parties themselves are often the initial source of the disinformation. Thus, my comments below will focus on foreign-propelled disinformation.

To determine how best to counter foreign disinformation, we need to first understand how our foreign adversaries create and spread disinformation. Those adversaries, especially Russia and China, engage in coordinated, integrated disinformation campaigns involving many elements of their governments. For example, when China decided to push the falsehood that its system of government was more successful at fighting the COVID19 pandemic than "weak, corrupt Western governments," the messaging started at the top, from the Ministry of Foreign Affairs, and was disseminated in a concerted way through the Twitter accounts of over 130 Chinese diplomats stationed around the world; Chinese-controlled news media and websites picked up the line and spread it too, and then seemingly corroborated it with further postings on social media and secondary news stories about how the message was reverberating around the globe. Russia's disinformation campaigns fomented by the GRU and other organs of the Russian state are if anything even more coordinated, so as to create the impression of an overwhelming number of "independent" news sources and social media accounts all espousing the Russian disinformation. In addition to creating inauthentic Facebook, Twitter and YouTube accounts owned by false personas (often with AI-generated fake profile pictures), the Russians might also enlist private sector proxies, such as the Internet Research Agency in St. Petersburg, to further promote the Russian falsehoods. The Russians careful monitor our domestic social media, seizing tendentious statements, conspiracy theories, and outright falsehoods, and then amplify and elaborate on them through their integrated disinformation machine.

This system of whole-of-government campaigns to promote online malicious disinformation is so different from our American values and the way our government operates abroad, that we have difficulty in appreciating the effectiveness of our adversaries' endeavors. And yet, to be successful in countering it, we must be equally integrated, and not regard online disinformation as a one-off expression on a particular social media account, or as something that can be simply rebutted with a press release from a government agency.

Thus, to fully apprehend, let alone effectively counter, the scope of foreign disinformation aimed at us, we need the active cooperation of the major social media platforms, the intelligence community and law enforcement to share current information about the sources and scale of disinformation campaigns. Artificial intelligence can clearly play a major role here in analyzing massive amounts of data on social media, combining information about foreign cyber activity from government and private sector sources, and in other ways assisting in the overall effort to identify and respond to disinformation. We would then be able to rebut falsehoods at an earlier stage, and that would entail consistent messaging from the White House, the State Department, the Departments of Defense, Justice and others. Our federal government has historically been reluctant to correct errors circulating in news media, let alone social media (partly out of First Amendment concerns and the restricted role of government relative to the private sector). But the efforts, for example, of the Department of Homeland Security in rebutting false claims—both domestic and foreign-sourced—of election fraud in last year's elections show how the federal government can make its voice heard in impactful ways. Moreover, if the federal government provides more detailed information to the news media, think tanks, cyber researchers and the like, they can be part of a national effort to stem disinformation.

While it is possible that some additional legal authorities may be needed on the margins (for example, mandatory reporting by private sector companies of foreign cyber maliciousness), the reality is that we can make much progress now, without new legislation, if the executive branch makes this a high priority and directs agencies to work together in a coherent way. Among other things, the intelligence community should be told that disinformation is a higher priority national security threat, additional resources should be dedicated for that purpose, and a greater effort can be made to declassify relevant information to assist social media companies in identifying and stopping foreign online malice.

These steps by the federal government, working with the private sector, are within our grasp and will help reduce the scope and influence of online disinformation. Obviously, the problem is complex, and other societal elements such as more civic education must be part of an overall solution—but the federal government can and should take the first critical steps now.

Mr. MOULTON. While I am concerned about military readiness, disinformation is clearly not just a military problem. As we face increasing efforts to mislead the American public and sow distrust and disunity, we see social media companies dodge substantive efforts to block disinformation's spread. If disinformation is not or cannot be eliminated, how would you advise we instead make ourselves harder targets? Ms. Jankowicz, you advise bringing local and Federal Government entities in health and education into the discussion. Can you describe in more detail how these departments and agencies might contribute to increased public digital literacy, which is clearly a matter of national security in addition to public health and public safety?

Ms. JANKOWICZ. Thank you for the question, Mr. Moulton. Building societal resilience at home is one of the most important aspects of responding to disinformation. Our adversaries use pre-existing fissures in our society—such as economic inequality, systemic racism, and hot-button issues like gun rights—to drive us further apart. Their efforts are amplified by broad-based misunderstandings of how the traditional and social media ecosystem operates. It can be difficult for national institutions to deliver resonant messages to the most vulnerable populations, however. Those that already distrust government are unlikely to be convinced by a public service announcement encouraging them to "take care before they share." This is where local government can play a critical role in building awareness of the tools and tactics of disinformation and building information literacy and civics more broadly. They can also serve as the connective tissue between funding sources and the organizations best positioned to deliver such interventions. I emphasize bringing state and local departments of health, education, arts, as well as local libraries to the forefront of America's counter-disinformation effort, because they know their local communities, their vulnerabilities, and the issues important to them best. In my research in Central and Eastern Europe, I have come across several local initiatives built on such bespoke local expertise. They include:

- In Estonia, where ethnic Russians and Russian-speakers are vulnerable to Kremlin-backed disinformation, the Integration Foundation offers free courses in Estonian language, cultural activities, and consultations about citizenship requirements both in Tallinn and Narva, a city on the border with Russia, where much of the ethnic Russian population is concentrated.
- In the Czech Republic, recognizing that the elderly are particularly susceptible to disinformation but hesitant to engage with counter disinformation programming, organizations attempting to build media literacy in the local population offered basic computer literacy training (such as how to use FaceTime to stay in touch with your grandchildren) and snuck in basic information literacy tenets to the curriculum. I call this the "peas in the mashed potatoes" approach.
- In the Republic of Georgia, one organization trains artists (singers, actors, musicians, comedians) from outside of the capital, Tbilisi, in recognizing and responding to disinformation. The artists then travel to their home region and put on a show incorporating what they've learned. This is "infotainment" at its best, delivered by influencers with credibility in an engaging and accessible format.

In the United States, state and local governments might fund similar programs. They could develop information literacy curricula to be delivered by local librarians (still highly trusted across the political spectrum). They might identify local civil society groups to partner with influencers with connections to the locality to act as trusted third-party messengers. In times of health emergencies, rampant democratic vulnerabilities, or developing public safety issues, such trusted conduits can be invaluable in getting authoritative information out to the public. It is important to recognize this approach is, by necessity, long-term. As I often remark, we cannot fact-check our way out of the crisis of truth and trust in which we find ourselves. But we can slowly build citizens' ability to recognize disinformation and introduce friction into the sharing process. Just like most Americans now know to ignore spam emails from purported Nigerian princes promising to make them millionaires, we can train them to spot and resist sharing the dubious information they encounter online. I am including several links to other writing I have done on this topic below. Thank you for the opportunity to testify on these important issues.

Mr. MOULTON. A third of troops have reportedly declined the Covid vaccine, undermining our troops' readiness well before we have entered into conflict. As I wrote in a recent Time magazine op-ed, this issue has demonstrated the ability of targeted disinformation campaigns to undermine troops' confidence in the emerging science and technology that underpin national security. How do you advise we protect troops from ongoing targeted disinformation campaigns and protect military readiness?

Dr. LIN. I agree entirely with your position that disinformation can be (and is indeed sometimes) a threat to military readiness. However, the DOD is not in a posi-

tion to protect troops from all sources of disinformation, simply because everyone, including troops, can obtain information from multiple sources. That said, the DOD does have control over a variety of information sources to which the troops may be exposed.

For example, cable television is available on many if not all bases. One could reasonably ask the question—which cable TV channels (or shows carried on those channels) broadcast large amounts of disinformation that are relevant to national security? For example, DOD would be fully within its prerogatives to forbid military bases from carrying RT (formerly Russia Today) on cable TV—and indeed, I have no knowledge that RT is carried on cable TV at any U.S. military base. But certain domestic cable channels have also carried programming with disinformation that threatens national security, such as disinformation related to Covid vaccines—and DOD has no obligation to make those channels (or shows) available on military bases either, even though off-base, everyone, including troops, has the right to access them as they see fit.

The same goes for Internet access provided on base. To the extent that the troops use DOD facilities to access the Internet, there is no reason that DOD should not block access sites that are known to provide substantial amounts of disinformation that threaten national security, even though DOD cannot forbid the troops from accessing such sites using their own resources (such as personal smart phones that they pay for themselves).

Both of these measures regarding cable TV and internet access on base require DOD to determine the nature of disinformation that is threatening to national security and to identify the channels and sites that are the most common purveyors of such disinformation. This will be an ongoing challenge rather than an assessment that can be done once and then left alone.

Such measures alone will not make a substantial dent in the problem that you describe. Over the longer term, I refer back to my testimony in which I call for DOD to take a more active role in training the troops on what it means to support and defend the Constitution against all enemies, foreign and domestic. Such training presupposes an ability to engage in critical thought and to have information literacy skills, and to the extent that these skills need to be strengthened in the troops, DOD has an obligation to address them in its training efforts.

Mr. MOULTON. Dr. Kirschbaum, it is my understanding that each of the services defines information warfare in varying ways, and therefore staffs and plans for information warfare differently. Does this limit our ability to effectively execute information warfare in a joint environment?

Dr. KIRSCHBAUM. There are indeed differences in how the services define and use terms related to operations in the information environment. The term "information warfare" technically is no longer part of joint doctrine and hasn't been since 2006. In its former definition, it covered activities DOD would need to perform to influence the actions of adversaries as well as the protection of our own information. It had both offensive and defensive elements. However, the context for its place in joint doctrine suggested that information warfare was something done in the early phases of a crisis or conflict. In other words, the perception might be that information warfare was something done only when there was a war. The broader term "information operations," on the other hand, had accepted that such activities could occur in peace and war. Some services or individuals continue to use the term "information warfare." The U.S. Navy, for example, has embraced the term in naval doctrine while also recognizing how its' sister services (U.S. Marine Corps and U.S. Coast Guard) use different terms and definitions (Operations in the Information Environment and Information Operations, respectively). The Navy's term implies more of a wartime set of activities, while the other terms imply broader application. But there is significant overlap. As we have discussed in this hearing, one of the fundamental challenges we face today is that activities, competition, and conflict are occurring every day globally. Our adversaries have prepared for this and view the information environment as a useful arena to pursue and secure their interests while degrading our own. This is particularly true in the area short of armed conflict (often referred to as the "gray zone"). Our adversaries operate freely in this space as we struggle to define the lines between peace and war where there may be none. While there is a large degree of generality and vagueness to the idea of the information environment, it is important to avoid confusion between the services and, more importantly, among combatant commanders about the importance of the information environment and our ability to operate effectively—in offense or defense. These definitions and other lexicon issues must be addressed if DOD is going to develop a cohesive, holistic, and joint strategy for Information (as a joint function); the Information Environment (i.e. current battle space); and activities, capabilities, operations, and security functions that will be employed in that battlespace. It is our under-

standing that officials within DOD understand this—as they have tried to thread this needle for years while struggling to update the 2016 DOD Strategy for Operations in the Information Environment. This will be an important part of the department's ongoing discussions about the right terms and the right context to ensure that the entire joint force can adequately plan for, and operate, in the information environment every single day.