[H.A.S.C. No. 115–92]

STATE AND NON–STATE ACTOR INFLUENCE OPERATIONS: RECOMMENDATIONS FOR U.S. NATIONAL SECURITY

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

HEARING HELD
MARCH 21, 2018

U.S. GOVERNMENT PUBLISHING OFFICE
30–562 WASHINGTON : 2019

COMMITTEE ON ARMED SERVICES

ONE HUNDRED FIFTEENTH CONGRESS

WILLIAM M. "MAC" THORNBERRY, Texas, *Chairman*

WALTER B. JONES, North Carolina
JOE WILSON, South Carolina
FRANK A. LOBIONDO, New Jersey
ROB BISHOP, Utah
MICHAEL R. TURNER, Ohio
MIKE ROGERS, Alabama
BILL SHUSTER, Pennsylvania
K. MICHAEL CONAWAY, Texas
DOUG LAMBORN, Colorado
ROBERT J. WITTMAN, Virginia
DUNCAN HUNTER, California
MIKE COFFMAN, Colorado
VICKY HARTZLER, Missouri
AUSTIN SCOTT, Georgia
MO BROOKS, Alabama
PAUL COOK, California
JIM BRIDENSTINE, Oklahoma
BRAD R. WENSTRUP, Ohio
BRADLEY BYRNE, Alabama
SAM GRAVES, Missouri
ELISE M. STEFANIK, New York
MARTHA MCSALLY, Arizona
STEPHEN KNIGHT, California
STEVE RUSSELL, Oklahoma
SCOTT DESJARLAIS, Tennessee
RALPH LEE ABRAHAM, Louisiana
TRENT KELLY, Mississippi
MIKE GALLAGHER, Wisconsin
MATT GAETZ, Florida
DON BACON, Nebraska
JIM BANKS, Indiana
LIZ CHENEY, Wyoming
JODY B. HICE, Georgia

ADAM SMITH, Washington
ROBERT A. BRADY, Pennsylvania
SUSAN A. DAVIS, California
JAMES R. LANGEVIN, Rhode Island
RICK LARSEN, Washington
JIM COOPER, Tennessee
MADELEINE Z. BORDALLO, Guam
JOE COURTNEY, Connecticut
NIKI TSONGAS, Massachusetts
JOHN GARAMENDI, California
JACKIE SPEIER, California
MARC A. VEASEY, Texas
TULSI GABBARD, Hawaii
BETO O'ROURKE, Texas
DONALD NORCROSS, New Jersey
RUBEN GALLEGO, Arizona
SETH MOULTON, Massachusetts
COLLEEN HANABUSA, Hawaii
CAROL SHEA–PORTER, New Hampshire
JACKY ROSEN, Nevada
A. DONALD MCEACHIN, Virginia
SALUD O. CARBAJAL, California
ANTHONY G. BROWN, Maryland
STEPHANIE N. MURPHY, Florida
RO KHANNA, California
TOM O'HALLERAN, Arizona
THOMAS R. SUOZZI, New York
JIMMY PANETTA, California

JEN STEWART, *Staff Director*
TIM MORRISON, *Counsel*
WILLIAM S. JOHNSON, *Counsel*
BRITTON BURKETT, *Clerk*

CONTENTS

STATE AND NON–STATE ACTOR INFLUENCE OPERATIONS: RECOMMENDATIONS FOR U.S. NATIONAL SECURITY

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
Washington, DC, Wednesday, March 21, 2018.

The committee met, pursuant to call, at 10:03 a.m., in room 2118, Rayburn House Office Building, Hon. William M. "Mac" Thornberry (chairman of the committee) presiding.

OPENING STATEMENT OF HON. WILLIAM M. "MAC" THORNBERRY, A REPRESENTATIVE FROM TEXAS, CHAIRMAN, COMMITTEE ON ARMED SERVICES

The CHAIRMAN. The committee will come to order.

Let me welcome and appreciate our witnesses for being here, as well as members and guests.

Whether the term used is "political warfare," "influence operations," "psycho-cultural warfare," "indirect warfare," "hybrid warfare," or one of the many others that have been suggested, it is clear that the United States and our allies are under consistent attack using non-kinetic tactics designed to undermine and weaken us.

We know that Russia intervened in a variety of ways to sow dissension during the 2016 election. History and now declassified documents establish that the former Soviet Union had a track record of active measures against NATO's [North Atlantic Treaty Organization's] deployment of intermediate-range missiles in Europe, for example, and those active measures included providing propaganda themes to peace movement groups, as well as organizational expertise, financial resources, forged U.S. military documents, et cetera, et cetera.

And according, again, to declassified CIA [Central Intelligence Agency] documents, that campaign was built upon a similar campaign they carried out against a proposed neutron bomb deployment in 1977 and 1978.

The point is it is all part of a standard playbook, and we should expect more of the same, including against decisions called for, for example, in the Nuclear Posture Review.

While most of the attention has been centered on Russia as a source of these attacks, they are not the only adversary using such methods. China has spent billions of dollars to gain economic leverage, buy access to infrastructure, and shape public opinion and perceptions around the world to its advantage. Iran, various terrorist organizations, and even North Korea make use of them as well.

These tactics challenge our traditional ways of thinking about warfare. They challenge our organizational structure on who is responsible for defending the country in this sphere. And they challenge our ability to develop and use tools needed to deal with them in a timely way.

As the National Defense Strategy says, "China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other nations' economic, diplomatic, and security decisions." And that was a quote. It is important for us to identify the motive behind these efforts, but the question remains whether we have the tools, the organizations, and the approaches to protect American sovereignty and national security.

We hope to gain insight into these issues from our distinguished panel of witnesses, but first, let me yield to the ranking member for any comments he would like to make.

[The prepared statement of Mr. Thornberry can be found in the Appendix on page 53.]

STATEMENT OF HON. ADAM SMITH, A REPRESENTATIVE FROM WASHINGTON, RANKING MEMBER, COMMITTEE ON ARMED SERVICES

Mr. SMITH. Thank you, Mr. Chairman. I agree substantially with all of your remarks about the importance of this.

It is a fairly simple process, and we are kind of failing at every level right now, in terms of our information operations. I mean, first of all, if you are going to engage in an information operation, you need to know what your message is. What is our message? What is it we are trying to convey? How are we trying to influence people?

Now, I think there are a couple very large issues there. One, we want to promote economic and political freedom as the ideal form of government and push that forward. We have not been conveying that message particularly well.

And I think the second piece is to counter extremism—and all forms of extremism. Certainly we are familiar with ISIS [Islamic State of Iraq and Syria] and Al Qaeda, but they are not alone in their extremist views. And it is not just peculiarly people who bastardize the Islamic religion; it happens in other religions and other ideologies as well.

So we need to be against extremism and for political and economic freedom. How do we communicate that? Well, to begin with, like I said, I don't think we have even sort of settled on that message. And then, second, once you decide what your message is, you have got to decide who your audience is. Who are we trying to persuade? And I think most important in that is, how do those people get their information?

So, ideally, if we have an information operation going on, we have got a message, we have an audience, and we have delivery mechanisms. And what has become clear is that the delivery mechanism right now is over the internet, is social media platforms, whether it is Facebook or YouTube or Twitter. That is what drives messages out there that get to people.

And, if nothing else, I hope that what the Russians have helped do is make us aware of how that works. I mean, because I think

there was an understanding that the internet was obviously a brand-new form of messaging here a couple decades ago, but we never really figured out how to use it exactly.

The Russians figured out how to use it. They figured out how to say, okay, this is our message, we are going to get it on the internet and get it on there in a way that it spreads. Part of that is setting up the bots, the automatic, you know, retweeting and sending out of information, but, beyond that, identifying sympathetic people. So you don't even have to do it through, sort of, fake or the bot approach; you simply find sympathetic people and then make sure you get your message to them and make sure that they spread it. The Russians have figured out how to weaponize the internet in an information campaign in a way that we did not.

We now have a template, as they, you know—I don't have any problem with imitating the Russians in terms of making use of these platforms. They have shown us how to do it. Now we just need to do it.

But we are not committed to that. And I think the largest problem is—there is a lot of commitment in this room. I think the members of this committee, I think the Members of Congress—you know, I haven't heard too many Democrats or Republicans who don't completely agree with all of this. What is missing is the executive branch. And they are really rather important in this.

The State Department, as near as I can tell, isn't even really engaging in an information campaign. And I know the Pentagon is trying, but this has to be a whole-of-government approach if we are going to be effective at it. And I think USAID [U.S. Agency for International Development] and some of our development efforts are important in delivering this message. And we are not there.

Now, I will just briefly touch on the sensitive topic before stopping, and that is it starts with the President. The President has been unwilling to do this.

Now, we can guess at a lot of different reasons for that. It seems like he is really worried about admitting at how good the Russians are at this for fear that somehow it will taint his election. As a Democrat, I want to say he won, okay? I don't question that at all, and really whatever any of his campaign officials were doing, what the Russians did matters just because they did it, even if there, you know, was or wasn't any collusion. We have got to engage in that. We have got to get the White House to decide that this is important and to engage.

More troubling is that the President doesn't seem to agree with the first part of that message that I said, that economic and political freedom matter.

Now, he got a lot of grief here recently for calling up President Putin and congratulating him on his election, which as—John McCain said it better than anybody. You know, the leader of the free world doesn't call up, you know, a dictator and congratulate him on winning a sham election. But it sort of undermines the political freedom message.

But more troubling to me was last year when the President called up President Erdogan in Turkey to congratulate him on the success of the constitutional referendum that they passed. And the

constitutional referendum that they passed was to clamp down on opposition, was to consolidate authoritarian power.

So does the President of the United States even agree with the message that political and economic freedom are things that we are supposed to promote?

And I understand it is complicated. There are times where we face threats. We have allies like Saudi Arabia and Egypt and elsewhere that are not necessarily engaging in what we want them to. How do you balance that? It is difficult.

But right now it doesn't seem like the White House is trying to balance it. They seem to be perfectly content to support the authoritarian approach. That is troubling, and we need to change that.

With that, I yield back and look forward to the testimony.

[The prepared statement of Mr. Smith can be found in the Appendix on page 54.]

The CHAIRMAN. Let me welcome our distinguished panel of witnesses.

We have General Philip Breedlove, former Commander of U.S. European Command and Supreme Allied Commander of NATO; Mr. John Garnaut, who is former senior adviser to Australian Prime Minister Malcolm Turnbull; and Honorable Michael Lumpkin, who is a former Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict as well as coordinator of the Global Engagement Center at the U.S. State Department.

Just because I mentioned a few formers doesn't mean these guys don't have a lot more in their bio, which was provided to all members.

Without objection, your full written statements will be made part of the record, and we would be pleased to hear any opening comments each of you would like to make.

General Breedlove, the floor is yours.

STATEMENT OF GEN PHILIP M. BREEDLOVE, USAF (RET.), FORMER COMMANDER, U.S. EUROPEAN COMMAND

General BREEDLOVE. Good morning, and thank you, Chairman Thornberry, Ranking Member Smith, and other members of the committee, for the opportunity to speak with you about Russian interference in democratic processes.

The Russian interference in the 2016 U.S. Presidential election is deeply troubling but not surprising. It is up to us as Americans to acknowledge the threats that Russian disinformation provides and to develop the effective strategies needed to combat them.

This weaponization of information by Russia is not new, as you have mentioned. In fact, it dates back to the Soviet Union. In 1983, a pro-Soviet newspaper in India published an article accusing the Department of Defense of creating AIDS [acquired immunodeficiency syndrome] in an attempt to develop new biological weapons. In 1964, the KGB [Russian Committee for State Security] used similar tactics in an effort to convince the Indonesian President that there was a CIA plot to assassinate him.

The primary differences between these disinformation campaigns and those of today is twofold. First, the internet and social media, as you have stated, make it so much easier to spread disinforma-

tion. And, secondly, these campaigns are increasingly targeting first-world Western nations.

Russia took full advantage of this new media landscape by promoting disinformation to sow discontent among Americans. It exploited divides in the American populace to promote what many have referred to as culture war. Surveys have shown that the U.S. is more polarized than it has ever been on issues such as gun control, immigration, religion, and race.

And Russian operatives, seeing an opportunity, have purchased social media advertisements and created profiles in order to promote partisan instances on their issues to further widen those riffs. Russian advertisements and profiles did not have a consistent political position. The only consistent aspect is that they all promoted partisan positions on immensely divisive issues.

The details of Russia's interference in the election are maddening; however, the reality is that we should not be surprised by this interference. The Russians have interfered with numerous elections in Western nations recently, including those in the Netherlands, Germany, and France.

There is increasing evidence that Russia worked to influence the referendum in which the U.K. [United Kingdom] decided to leave the European Union [EU], as recently shown in a Senate Foreign Relations Committee report. It has promoted anti-immigration sentiment in Europe by creating and spreading the story of "Poor Lisa," a 13-year-old girl who, as the fallacious story goes, was abducted and raped by migrants.

Further, we ourselves have meddled in elections in our own way, and we have to face those facts. In 1953, Allen Dulles offered $5 million to an agent to sway the Filipino elections. In 1958, Operation Booster Shot encouraged rural Laotian farmers to vote against communist politicians in Laos.

Our meddling did not end with the Cold War. In the 2006 Palestinian elections in Gaza, the United States provided economic assistance in an attempt to bolster Fatah's chances. The reality is that both the United States and Russia have meddled, and we should not be surprised if the trend continues.

What is astounding about Russian meddling is how brazen Russia has been in executing it, as well as the fact that Russia seems to believe that it can escape this with its reputation unsullied. Russia appears to be surprised by the outrage that has been seen throughout the U.S. The U.S. has been a leader and a pillar of Western democracy, and the fact that Russia believed that it could interfere with American elections with no response is what is shocking to me.

However, Russia's interference in the 2016 U.S. Presidential election is merely a symptom of a larger hybrid war against the West, in which economic, cyber, and disinformation tactics are used in conjunction with conventional forces in order to exert force or pressure on an adversary.

In February 2013, General Valery Gerasimov, chief of the general staff of the Armed Forces of Russia, gave a speech entailing this strategy. He claimed, "The very rules of war have changed. The role of nonmilitary means in achieving political and strategic goals has grown. In many cases, they have exceeded the power of

force of weapons in their effectiveness. The focus of applied methods of conflict has altered the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures, applied in coordination with the protest potential of the population."

This has led to the coining of the term the "Gerasimov Doctrine." This describes Russia's view that warfare is not simply a conventional affair but one that uses the aforementioned cyber, economic, and information tactics. This is notable because it shows Russia acknowledges that its election meddling is a form of warfare. While Russia may deny that it interferes with elections or claim that it is innocuous, the words of General Gerasimov ring loud and clear: Disinformation efforts are efforts of warfare.

The reality is that Russia is using hybrid tactics to target Western values, democratic governments, and transatlantic institutions. President Vladimir Putin claimed in a state of the nation address that the collapse of the Soviet Union was a major geopolitical disaster in the 20th century.

Russia sees the West, and in particular a unified West, as an adversary. Waging a conventional war against the West would be unfavorable to Russia. As such, it has used hybrid warfare to break up Western unity.

Exploiting divisions in U.S. society and promoting a culture war is one key element of Moscow's efforts to weaken the West. Through disinformation, it has plied differences in Europe to promote Euroscepticism and to grow the notion among the peoples of Europe that the EU is not beneficial. It has waged cyberattacks, such as the NotPetya attack in Ukraine in 2017, the Fancy Bear attack of German members of parliament earlier this month, or the numerous distributed denial-of-service attacks on the Estonian Government.

It has used economic subversion to exploit the relatively smaller economies of neighbors to subvert political power. Russia uses its vast energy resources to promote the dependence of its smaller neighbors, working to keep them in a Russian sphere of influence and preventing them from turning to the West.

The Russian interference in the 2016 U.S. Presidential election has received an unprecedented amount of media coverage. However, we should not be so limited as to see this interference in a vacuum. In order to effectively combat this interference, we need to understand the scope of Russian hybrid warfare. We need to view this as a comprehensive problem that connects the dots of recent Kremlin activity. We cannot simply take a stance against a specific case of election interference; we must take a stance against Russian hybrid warfare in its entirety.

In all the cases of Russian disinformation and election interference, the West has been slow to see it and even slower to react. We need to move past simply trying to formulate a reaction to interference in this election, and we need to move to a place where we are ready to combat hybrid warfare and get past reacting.

Hybrid warfare is a form of warfare that the United States has yet to fully understand, never mind prepare for. The revelation of Russian disinformation in the election is a wake-up call that hybrid warfare is occurring, even if we are unwitting.

Simply condemning the election meddling is not going to solve the problem, and it is not going to prevent future Russian hybrid operations. We must treat this with the gravity that it deserves. We need to take a position, establish policy, and then execute it.

The Russian hybrid threat is larger than the election and larger than the United States. It is a threat to the liberal order that the West has become accustomed to, and it will continue to be until we develop an effective strategy and implement the necessary policies to combat it.

Sir, thank you, and I look forward to your questions.

[The prepared statement of General Breedlove can be found in the Appendix on page 56.]

The CHAIRMAN. Thank you.

Mr. Garnaut.

STATEMENT OF JOHN GARNAUT, FORMER SENIOR ADVISER TO AUSTRALIAN PRIME MINISTER MALCOLM TURNBULL

Mr. GARNAUT. Thank you, Chairman Thornberry and Ranking Member Smith, distinguished members. Thank you for having me along today.

Is this microphone okay?

The CHAIRMAN. If you could just speak directly into it, because it is directional, and so if it is off to the side, it doesn't work as well.

Mr. GARNAUT. Sure. Thank you.

To understand the mechanics of China's international influence, we have to look beyond the gravitational pull of the Chinese economy and the warfighting power of the People's Liberation Army. That is what we usually focus on, and they are both important, but, to me, the more interesting and the more important space is in between those two poles, and that is the space of influence and interference.

This is the space where the Chinese Communist Party manipulates incentives inside our countries in order to shape the conversation, manipulate perceptions, and tilt the political and strategic landscape to its advantage.

The party works relentlessly to find common interests and cultivate relationships of dependency with its chosen partners. The modus operandi is to offer privileged access, to build personal rapport, and then to reward those who deliver. From open-source materials, we can see this happening in universities, in business communities, in ethnic Chinese diaspora communities, in media and entertainment, and also in politics and government itself.

But the institutions and ideologies and the methodologies are so alien to our systems, we are having trouble seeing it, let alone responding to it. The party has, to use its own terms, been winning without fighting.

However, under the uncompromising leadership of President Xi Jinping, China's activities have become so brazen and so aggressive that we can't ignore it any longer. A reevaluation is taking place across half a dozen democracies in the world, including the United States and Australia, and this conversation is now taking root in many other countries as well.

I have described the Australian experience in an article this month in Foreign Affairs magazine, which I have attached to my written submission. I won't duplicate that here, but I want to underscore what I think is the most important message from the Australian experience. And that is the importance of having analytical clarity, of working with principles, and responding with strategy.

Our challenge, and the challenge of democracies across the world, is to work with the strengths and shore up the vulnerabilities of our open, multicultural, democratic systems. We need a rigorous and principled approach that is capable of supporting a broad and durable consensus within countries and between countries. We need to conceptually separate the black, the covert, from the white and recognize that there is a large gray area of ambiguity and plausible deniability that sits in between.

This process requires a great deal of empirical work, both in and outside government. But once we have the empirical baseline and we have worked out which activities we care about and how much we care, then we can start to formulate and design a surgical response that manages the risks and targets the harm without harming ourselves.

In my view, we should continue to welcome ordinary diplomacy and public diplomacy and economic activity that does not come with strings attached. But wherever there is covert, corrupting, or coercive behavior, when the legitimate and transparent influence processes cross the line into harmful interference, then we need to be uncompromising, ourselves.

Shutting down the black—the covert, the coercive, the corrupting—is primarily a counterintelligence and law enforcement challenge, a very big one, but it won't be enough on its own. We also have to build transparency and accountability mechanisms to illuminate the gray. We need to reinforce and reactivate the natural antibodies of our civil societies, the natural antibodies that the party, the Communist Party, has been working to suppress and, in some cases, disable.

In Australia, the Turnbull government has been developing a counter-interference strategy that is built upon the principles of sunlight, enforcement, deterrence, and capability. The strategy is country-agnostic in that it is designed to apply to any country that misbehaves, not just China. And the strategy includes new legislation that is targeted at both the black and the gray.

One set of laws introduces tough but graduated criminal provisions against political interference and espionage. Another set of laws imposes disclosure obligations for those working in Australian politics on behalf of a foreign principal. This is an updated transparency regime which is loosely modeled on your Foreign Agents Registration Act.

Importantly, enforcement activities are also being brought within a central, integrated hub.

But this is only the very early stages of a long struggle to reinforce the integrity of our democratic processes. There is an enormous body of work that needs to be done, and I am looking forward to this discussion.

[The prepared statement of Mr. Garnaut can be found in the Appendix on page 62.]

The CHAIRMAN. Thank you.
Mr. Lumpkin.

STATEMENT OF HON. MICHAEL D. LUMPKIN, FORMER ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS AND LOW-INTENSITY CONFLICT, U.S. DEPARTMENT OF DEFENSE, AND FORMER SPECIAL ENVOY AND COORDINATOR OF THE GLOBAL ENGAGEMENT CENTER, U.S. DEPARTMENT OF STATE

Mr. LUMPKIN. Chairman Thornberry, Ranking Member Smith, and distinguished members of the committee, thank you for the opportunity today to address you on the topic of state and non-state actor influence operations.

I believe the Congress has correctly identified such information operations as an ongoing and persistent threat to U.S. national security interests. Unfortunately, based on my previous experience in government, I am similarly convinced that we have quite a ways to go before we actually get it right in order to protect and defend those national interests in the modern information environment.

Since the end of the Cold War with the Soviet Union, which arguably was the last period in history when the U.S. successfully engaged in sustained information warfare and counter-state propaganda efforts, advances in technology have enabled instantaneous global communications. We are living in a hyperconnected world, where the flow of information moves across borders in real time and across traditional and social media platforms.

The lines of authority and effort between public diplomacy, public affairs, and information warfare have blurred to the point where, in many cases, information is consumed by U.S. and foreign audiences at the same time via the same methods.

While the means and methods of communication have transformed dramatically, most of the laws and policies governing how the U.S. Government responds to sophisticated operations and disinformation campaigns by foreign adversaries have remained largely unchanged. It is true there has been some tinkering, there has been some tweaking, but nothing substantive or transformational. Simply put, our institutions have not kept pace with the evolving threats.

Antiquated bureaucratic structures and traditional lines of authority remain a significant impediment to progress. To date, there is not a single individual in the United States Government below the President of the United States who is responsible for managing U.S. information dissemination and providing strategic guidance for how to confront our adversaries in the information environment.

While the 2017 National Defense Authorization Act mandated that the Global Engagement Center, or GEC, lead, organize, and synchronize U.S. Government counter-propaganda and disinformation efforts against state and non-state actors abroad, it failed to elevate the head of the GEC to a position of authority commensurate with its expansive mission.

The GEC operates at the assistant-secretary level and lacks the necessary authority to direct the interagency. In practice, this means that the GEC is considered, at best, a peer to a half-dozen

regional or functional bureaus at the State Department and numerous disparate organizations at the Department of Defense. Needless to say, the other departments have equity stakes in this space as well.

Simply put, although the GEC is directed by law with the mission to lead interagency, the practical reality is that its role is reduced to simply suggesting function, which agencies can choose to follow or not to follow as they see fit. The result is a significant misalignment of responsibility, authority, and accountability which will continue until this is changed in statute.

It is not unreasonable to think that the U.S. will always be at some disadvantage against our adversaries in the information environment. We are a nation of laws, where truth and ethics are expected, and rightly so. Our enemies, however, aren't facing the same constraints. Our adversaries, both state and non-state actors, can and will continue to bombard all forms of communication with their messages in attempts to influence public perception, create doubt of our actions or intentions, and recruit people to their cause.

We must ensure that we organize U.S. Government efforts in such a manner that maximizes desired outcomes through discipline, agility, and innovation.

Again, thank you for the opportunity to be here today, and I look forward to your questions.

[The prepared statement of Mr. Lumpkin can be found in the Appendix on page 76.]

The CHAIRMAN. Thank you.

I will just mention that a number of members of this committee are also members of the Foreign Affairs Committee. And looking at the issue that you mentioned about the appropriate level of the director of the Global Engagement Center is something, I think, that a number of members probably should look at on both committees because it is their jurisdiction.

I think a lot of the questions that you all are going to get are going to be about what we do, but I want to just take a moment to shine a little brighter light on what is happening, because I think understanding is really critical as a first step.

A lot of attention, as we all know, to what happened in the 2016 election. And so there are recommendations, even this week, about shoring up our electoral process.

I don't think there has been as much attention devoted to these other countries trying to influence our decisions. And I mentioned, as did General Breedlove, some of these efforts in the past, to prevent us from deploying the Pershing II and the GLCMs [ground launched cruise missiles] in the 1980s or the neutron bomb in the 1970s, that they are continuing to be involved—have been involved historically in trying to make sure that we didn't make national security decisions that would run counter to their interests.

And so that is the reason, when I think about the Nuclear Posture Review, or various other funding decisions that this committee has to make, I worry about those attempts continuing but us not recognizing it.

General Breedlove, could you elaborate just a little bit, because you have been on the front lines of this, about, in your case especially, the Russian attempt to not just influence our elections but

influence the political decisions we make, especially in the area of national security?

And then, Mr. Garnaut, if you could help us think about the ways the Chinese are attempting to influence not just our elections or our perception of them but the decisions we make that affect national security.

General Breedlove.

General BREEDLOVE. Thank you, Chairman.

And I completely agree with the statement before your question. I would point out, for instance, what happened when Russia first went into Crimea and then into the Donbass. Russia clearly had a very localized overmatch when it came to military forces, but if all of NATO awakened, it could rapidly have changed. And so what we saw was a campaign that started immediately with very bellicose talk, to include what I have called in this room before loose talk about nukes, in order to try to influence the decisions of the West about how they would respond to what was going on.

So, very broadly, in cases like the Ukraine, they have tried to influence us. And I would also say that some of the actions early in Syria are of the same ilk. The long-range shots out of the Caspian Sea into Syria had very, very little tactical effect, and I think they were mainly taken to show the West, "Look, we can range your capitals from the Caspian Sea. Don't mess with us."

And so I think in every case, as we look at application of Russian capabilities, we need to have our eyes open to a broader message, because they are trying to, as you said, Chairman, influence our decisions in these spheres.

The CHAIRMAN. Thank you.

Mr. Garnaut.

Mr. GARNAUT. Yeah, there are lots of parallels between Russia and China. They are fascinating, and sometimes they are illuminating.

One of the parallels is the effort to fragment alliance systems. So, certainly in Australia and elsewhere, there is a huge amount of effort to weaken the commitment of allies to the United States and to each other.

And part of that, I think, is quite a sophisticated messaging system which is kind of inconsistent when all together but you can see how it works. And one is the message that China is inherently and possibly uniquely peaceful; you don't need to set up your armed forces because they are peaceful. That is it.

Two, the second message is that China's rise is inexorable. So, even if you don't like it, there is nothing you can do. Resistance is futile.

The third message, which is contradictory to the first but it comes out from different channels, back channels, and is really important when targeted at certain times, is that, actually, China is really dangerous, and it is ruthless, and if you get in the way, it is going to really hurt.

And so it is this orchestra of messages which has worked to manipulate the public opinion, elite opinion backdrop and the mental wallpaper of decisionmakers as they are making decisions about their own force capabilities and build-up and the commitment to the U.S. alliance system and other security partners.

The CHAIRMAN. That is helpful. Thank you.

Let me yield to Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman.

And I will go where the chairman suggested. What could we be doing better? Or, put differently, if you were to say, "Here is the plan," and you could walk over and be God for the moment in the White House in terms of how we do a better job of countering all of this very aggressive messaging that the Russians, the Chinese, and the extremists are pushing, how would you organize that as a starting point? Who in our government plays the most important role? White House? You know, NSC [National Security Council]? Pentagon? State Department? What would the team look like?

General BREEDLOVE. Congressman, so let me take the first stab at it. And I may or may not actually hit what you are shooting at, but I want to offer that we are here sort of talking about the information piece of this conflict that we are in. And I think, first and foremost, we need to recognize that we are actually in a conflict.

The second thing I would offer in how to organize our response is to understand that our opponent is broadly attacking us. I use that very simple model, DIME—diplomatic, informational, military, and economic—to describe a nation's power. There are much more sophisticated models, but for a fighter pilot that works.

And what we see is our opponent is attacking us diplomatically at the values that we have and our legitimacy in the West. It is attacking us, as we have talked about in this committee, in the information space in incredible ways. In Europe, Russia is now using force again to change internationally recognized borders. And then Russia, as we talked about, is using its economic sphere to influence pricing and availability of fuel to nations that need it. So——

Mr. SMITH. I am sorry, but that is not what I asked. It is all very helpful, but we have heard that. What would the team look like?

I mean, if I can just give you an analogy——

General BREEDLOVE. Sure.

Mr. SMITH [continuing]. That I think worked for us. After 9/11, General McChrystal kind of led the notion that we are being attacked by a network, and it takes a network to beat a network.

So, A, we went to an elaborate effort to understand what that network was that was attacking us, and then we built our own network. And all over the world, every morning, all the different pieces of that—and I won't get into all the different pieces of it—got together at 7:00 a.m. east coast time and said, how are we doing, what is going on here, what is going on there, what piece of it do you have, FBI, whoever.

You know, I think we need that type of comprehensive approach. And I just want, what is the first step? What is the building block to build that counter-narrative?

General BREEDLOVE. Slow to get to my conclusion, which was we have to have an all-of-government response, and that has to be led somewhere, either an empowered GEC to bring all of government together or an entity in the NSC to bring all of government together. But we need to respond in an all-of-government way.

Mr. SMITH. And right now it is fair to say nobody is in charge, right? There are some people doing a few things here and there,

but there is no person who is like, I get up this morning, my job is to counter this information campaign?

General BREEDLOVE. I think that is correct.

Mr. SMITH. Okay.

Mr. LUMPKIN. And, sir, if I could add——

Mr. SMITH. Yes.

Mr. LUMPKIN [continuing]. I kind of think of the information space as we have an orchestra; what we don't have is a conductor. And we need to have a single person that is held accountable for U.S. Government information efforts.

Mr. SMITH. Just quickly on that piece, since there are kind of, like—there are several different pieces here. One, obviously, is the, you know, Russia—well, there is Russia and their efforts to undermine democracy and freedom. There is China and their efforts to do the same. There are the violent extremist groups that we are trying to counter. And then there is what the chairman mentioned, is the collective effort to, you know, interfere in our politics, not just in the elections but in our decision-making process.

Is it possible, do you think, to wrap all of that into one thing and say, "Okay, you are in charge, here is the information warfare, you have got to cover it all"?

Mr. LUMPKIN. I think what we have done as a nation correctly is we created the Director of National Intelligence to get 17 intelligence agencies together kind of marching in the same line.

And they also advocate for budgets, resourcing, legislation, people. I mean, again, I always can tell people's priorities by where you put your resources, your people, money, and your time.

And I would offer that we don't have a whole-of-government approach to this. When I took over the GEC, we had a $5.6 million base budget.

Mr. SMITH. Yeah. Thank you.

Mr. GARNAUT. If I could add just to that, from the China angle, they are very good at playing off the different silos of our systems against each other.

So if I can only underscore what General Breedlove was saying about the importance of elevating this issue and making it very clear the strategic importance of this issue, and then decisions flowing down to each part of our system, rather than the individual bureaucracies and agencies coming up with their own solutions and trying to sort of horse trade at the top.

Mr. SMITH. Okay.

Thank you, Mr. Chairman. I yield back.

The CHAIRMAN. Mr. Conaway.

Mr. CONAWAY. Thank you, Chairman.

Our Intel Committee will release tomorrow, we think, our findings and recommendations of what we thought the Russians did or didn't do pertaining to our elections and the systems that we have in place, the voter registration and the tallying systems. All those kind of things are a little more mechanical.

The real fight is, as the chairman may have said and General Breedlove said, is between the ears of Americans, and how do you protect. Jefferson wrote extensively about how valuable an educated public is to the preservation of democracy.

And I am looking right now at RT America—RT, Russia Today—which is a Putin tool to propagandize in America. And Jesse Ventura has a show on there, Ed Schultz has a show on there, Larry King has a show on there. I assume they know who they are working for, but the American people may not.

So we, how do we—and this is more just a statement than a question, but the real issue for us is how do we make sure that Americans aren't improperly influenced? In a free society with a free press where anybody can get access to these channels, how do we make sure Americans understand who they are listening to, who they are being influenced by?

Because at the end of the day, Putin's real issue was, can I get somebody to vote differently than they would otherwise have voted had I not engaged in this fight?

And that is, you know, probably not an Armed Services Committee circumstance, but helping the American people understand where the risks are, looking at—you know, like, RT, you pull it up, it looks like it is a regular, legitimate American news source, when the truth of the matter is at its core is a Putin-driven propaganda machine.

Just a statement, Mr. Chairman. I don't have much of a question in that regard, because, really, this issue is more how do we make sure Americans, when they go to the polls, have in mind the right person to vote for, or against, based on legitimate sources.

So if any of the three have a comment in that regard, I would be happy to listen to you.

All right. I yield back. Thank you.

The CHAIRMAN. Mrs. Davis.

Mrs. DAVIS. Thank you, Mr. Chairman.

And thank you to all of you for being here. I really appreciate your remarks. I think we all do.

You have talked, and certainly Mr. Lumpkin, you have talked about the Global Engagement Center and you have talked about the need for a conductor. But where is the executive in this? How important would the executive be to an elevated and empowered GEC? And could it actually not be that important if it wasn't seen as critical to the country?

Where does it stand?

Mr. LUMPKIN. Well, I mean, I kind of scratch my head sometimes, wondering, you know, where is the executive right now in this process.

I mean, I think what we see is the—I mean, information operations are military operations, just—you know, information operations to support, you know, military objectives.

We have the public affairs team out there, you know, messaging to the American population. We have the State Department, who is focusing on the public diplomacy, which is influencing populations abroad. The gaps and seams in those are massive.

And not only do you have the gaps and seams between them, but you have the hyper-connected world where what goes on in the public affairs is reached near simultaneously internationally. What happens in country X affects—it hits the American populations.

So the world has changed on how we can consume, manage information and what flows where, but our silos are still there. Our silos still exist.

And this committee, in conjunction with their counterparts in the Senate, have done some tremendous work in the 2017 National Defense Authorization Act. In fact, it took the Armed Services Committee to legislate in the State Department on how they manage information, because it wasn't getting done.

So I do think it starts here, to get the executive going in the right direction. But I think it is time to do a holistic look as far as how we manage information. It may be time for, you know, a control-alt-delete and look at new ways to do business. And I think elevating the GEC or a GEC-like element may be the right course of action.

Mrs. DAVIS. Uh-huh.

General, did you want to respond——

General BREEDLOVE. Just——

Mrs. DAVIS [continuing]. On where do we start?

General BREEDLOVE [continuing]. A small add-on.

I really liked the words Mr. Garnaut used. This should be a top-down-driven thing. It doesn't have to be the executive, but if it is not the executive, then the executive needs to empower someone below them, give them authority, responsibility, and accountability for the mission and then tell them to move out.

Mrs. DAVIS. Mr. Garnaut, did you want to respond?

Mr. GARNAUT. No, I won't add to that.

Mrs. DAVIS. All right. Great. Thank you.

As you know, the whole-of-government approach that we tried to work with after 9/11 was—how do you think that that was transformative on some levels? What did we accomplish—why did we accomplish that and not accomplish other things?

Mr. LUMPKIN. I think it is, first of all, there was an immediate call to action because of the event that happened, because the horrific nature of what 9/11 did to the psyche of the American people, as well as physically damaging and hurting families and the American people writ large.

Until we have that—I have learned that policy generally doesn't make itself. You need a forcing function. I would like to think that people are awake enough, based on what has happened and what is happening in the information environment, that it is time to do something about it before something horrific does happen.

Mrs. DAVIS. Uh-huh.

I am thinking also about our relationships with our NATO partners. And, certainly, General Breedlove, you were very involved with NATO. We know that, in many ways, it is really our Western—Western nations are strong, but that also makes us susceptible, because of our institutions.

How do you think we do address these issues with our partners without compromising those values?

General BREEDLOVE. So let me agree, Congresswoman, with something you said which is important. And sometimes our strengths, which are our freedoms and our values, make us vulnerable. We are not accountable to the truth in the way we operate

in these public spaces, where—or, we are accountable to the truth in these public spaces, while our enemies are not.

And so I am not in favor of stooping to the wrong type of tactics in reply and compromising our strengths. And that is what I see in NATO as well. Western democracies, Western values, Western institutions are one of the first targets of these kind of efforts coming from our opponents.

Mrs. DAVIS. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Mr. Wilson.

Mr. WILSON. Thank you, Mr. Chairman.

And thank each of you for being here today. We appreciate you highlighting such important issues that have been a great concern of the committee over years.

One issue in particular that I recognize is working on China's ongoing influence campaign through the establishment of Confucius Institutes across the United States.

Currently—and this is a question for each of you—there are 103 active Confucius Institutes that were described in 2009 by Li Changchun, the head of propaganda for the Chinese Communist Party, as, quote, "an important part of China's overseas propaganda setup," end of quote.

It is for this reason that yesterday I introduced legislation, H.R. 5336, the Foreign Influence Transparency Act, which would require transparency of these institutes through modifying the Foreign Agents Registration Act for disclosure.

Do you believe it is appropriate to require organizations like the Confucius Institutes to register under the Foreign Agents Registration Act?

And, additionally, it has been 23 years since the Foreign Agents Registration Act, FARA, has been last updated. What recommendations would you give to the committee on how it should be changed to deal with Confucius Institutes or other influence operations that you have discussed today?

Mr. GARNAUT. Well, thank you. And I did note those reports with interest.

Now, Australia has had a close look at your FARA legislation. We didn't have any before, so we are coming from a standing start. And I think what we have tried to do in Australia is to broaden the definitions a little bit to account for the fact that a lot of foreign interference is indirect. You know, FARA tends to be focusing on a more contractual relationship, so you need to have some broader definitions.

And I think that the direction you have taken with that draft legislation is very encouraging. And leaving aside whether or not the Confucius Institutes themselves should be registered, I think that is the right direction.

Because what they do is partly propaganda, but I think even more important is their connection to the United Fronts Work Department system. And that is that, you know, they can potentially be used, or we need to stop them being used, as a platform within universities for influencing decision making in universities, as well as having an element of propaganda in itself.

I think your expansion of the FARA legislation is certainly a very encouraging thought.

Mr. WILSON. Thank you.

Mr. LUMPKIN. I absolutely agree. I think we need to look at the definitions within the FARA to see what is included and what is not and maybe take a fresh look at them. But the legislation at first glance looks really, really good, so I am pleased you did that. Thank you.

Mr. WILSON. Thank you.

General.

General BREEDLOVE. Sir, just to save your time, I would just completely align myself with the concept of transparency.

Mr. WILSON. Thank each of you for that.

And, Mr. Lumpkin, given your previous experience as Special Envoy and Coordinator for the Global Engagement Center, could you inform the committee as to ways in which this committee can support their mission, whether it be increased authority, funding, or coordination with SOCOM [U.S. Special Operations Command] in their counterpropaganda efforts? Do you believe more can be done to ensure their success? As I believe their mission is absolutely critical.

Mr. LUMPKIN. I do. Thank you.

I think one of the pieces, as I mentioned, is that they need to be fully empowered to effectively execute across the interagency, to include USSOCOM as one of the combatant commands.

I additionally believe they need to be resourced, not only with money but with people and with leadership. Since my departure in 2017, there has been an Acting Special Envoy, and I would like to see somebody permanently put into that place to guide that institution.

But I do think that one of the key pieces is to elevate them to the point where they can have a compelling and effective voice. I think the other piece the committee could do is—hearings always assist in transparency, so I think that hearings on subjects like this one go a long way in moving forward.

Mr. WILSON. Thank you very much.

And, General Breedlove, the Governments of the U.K., U.S., France, and Germany have recognized the use of the nerve agent Novichok as an offensive use of weapons.

Do you believe that the use constitutes an act of war? If so, what should the U.K. or allies do to reciprocate?

General BREEDLOVE. Thank you for the question.

And I quickly found, when I was the head of NATO, I couldn't determine what was an act of war. The NACC [North Atlantic Cooperation Council] got to do that. But I would definitely construe it as a warlike action on a friendly soil.

And I think that the more surprising piece of this is, again, how brazenly and how open these actions were. And I think that we have seen actions like this in our own capital in the past, and so these are concerning.

Mr. WILSON. Thank you all.

The CHAIRMAN. Just briefly, on the funding for the Global Engagement Center, Mr. Lumpkin had mentioned $5 million previously. As I understand, in the omnibus there is the authority to

transfer up to $60 million of DOD [Department of Defense] money for specific projects in the Global Engagement Center, and then, of course, what State Department puts in. So just to let everybody know, again, it is—DOD money can be transferred as well as the State money.

Mr. Larsen.

Mr. LARSEN. Thank you, Mr. Chairman.

Mr. Garnaut, first off, congratulations on winning the Brownlow Award in 1993 as the best and fairest player in the Australian Football League. Having grown up watching the early days of ESPN and a lot of Australian football, I didn't know there was a fair way to play it, and I am glad to know that there is. So congratulations.

And for you, as well, because of your experience in Australia, one of the concerns I have about how we are approaching the relationship with China is that we have a defensive playbook and not an offensive one. We are not filling gaps that China is filling, where we can fill those gaps. And one of them has to do with the Confucius Institutes issue.

And I am wondering—I think another way to approach the Confucius Institutes is to actually identify these universities and maybe expand Federal funding for Chinese language and Chinese culture for students so that they don't have to outsource that activity to Confucius Institutes.

And I am wondering in Australia what you are doing, since you mentioned in your testimony that universities, I think, need new processes and transparency to deal with Chinese influence on campuses. How are you approaching that there?

Mr. GARNAUT. Well, you have hit upon a key vulnerability here. China is really filling—providing a service that we are failing to provide, and that is China capability—linguistic capability, understanding of Chinese contemporary politics and history. So the Confucius Institutes have found a kind of, you know, great black hole that they can fill.

So, yes, we do need to work hard on rebuilding our China capability—I think that applies to the United States as well as Australia—at universities.

I would just flag one thing about the Confucius Institutes, which is at least we know about them and people are talking about them. And, in a way, that degree of transparency goes a long way to curing the problem. What I am personally more concerned about is things that, you know, don't have a big flag over their building. So we see other institutes and research institutes performing similar functions but without the attention, and I think that is where we need to pay a lot more attention.

But transparency is absolutely key. I think we are unanimous on this panel. Inside universities, I can think of a couple things to do. And, you know, in many cases, it is up to the universities themselves, but I think there is a lot more room for transparency about the sources of funding, particularly donations. We should be honest about the political connections of money that comes. We should have more transparency about who is funding research projects—who exactly is funding research projects and, also, who is funding trips to China. You know, the junket trade is rife. We just need

to—we don't want to stop it, but we need to flag it when it is happening.

Mr. LARSEN. Yeah. Great.

And I want to follow up on the point you made about consistency and really giving that message from the top down.

So, here in the U.S., we have just—one agency has concluded that the Belt/Road initiative [BRI] is a tool of domination for the Chinese, while another Federal agency is actively trying to find ways for U.S. businesses to participate in Belt/Road projects. That seems to be, to me, inconsistent. And we can decide which one we ought to choose, but it is just flat-out inconsistent.

Again, thinking about going on offense—and maybe Australia has looked at this question—what can the U.S. do to compete or at least have a presence in those places where China's BRI has a presence, as opposed to just saying we are going to try to ignore it, put on blinders, think it doesn't exist, but actually have a presence in these same places where BRI is being implemented?

Mr. GARNAUT. Yeah. The policy responses to BRI have been disjointed all around the world. And, typically, economic agencies will support it—you know, they see the idea of building things and making things to be a good thing—and security agencies don't. And often it is a very messy, unmediated response that happens. We see that from a lot of countries around the world.

So, yes, that does highlight the central importance of elevating China and Russia policy to a higher level and pushing down the objectives and the strategies.

With BRI, obviously, again, they filled a vacuum. You know, if we are, between us, no longer supporting development in the way that we used to in my part of the world, in Southeast Asia and the Pacific, well, it provides opportunities for others.

So I think that there is opportunity to do more there but, also, really to focus again on transparency. Because if we can just empower civil societies to do a better job, to do more of what they are doing—local communities, local media, local journalists—sunshine will cure a lot of the harm that we are worried about.

Mr. LARSEN. Thank you very much.

Thanks, Mr. Chairman.

The CHAIRMAN. Mr. Lamborn.

Mr. LAMBORN. Thank you, Mr. Chairman. Thank you for having this important hearing.

And I am going to make an editorial comment real quickly before I ask my question of the witnesses. And that is, no matter what the President does or doesn't do, he is going to be criticized. If he doesn't congratulate Putin, some people would say he is not reaching out, he is going it alone, et cetera, et cetera. So I just want to defend the President by saying it is important to take some of the criticism with a grain of salt.

Okay. To my questions of the panel.

You have already been asked about China, and you have talked a lot about that. I want to follow through a little more on that. What happens to democratic institutions in the United States and in Australia if we don't push back on the kind of influence that they are trying to exert on our political institutions as a democracy?

Mr. GARNAUT. I might have first crack at that.

Well, you lose control of the debate.

So, in China's case, one of the things that we have just failed to recognize and failed to address for decades, and it has allowed the problem to fester, is the extent to which China or the Chinese Communist Party has been able to co-opt friendly voices in the Chinese community, the Chinese media in our countries, and to coerce and intimidate others out of participating in the debate. So it rewards and nurtures favorable conversations and shuts down others.

So we really need to go and protect people and provide safe spaces for people to have their freedom of expression, which the rest of us have taken for granted. And now we are seeing that modus operandi spread out of the Chinese communities into the mainstream. And so we are seeing major efforts by China to intimidate publishers, journalists out of participating in the conversation and to reward others. You know, they help you succeed. They find a favorable sympathizer, and they help you succeed.

We need to balance that. We need to protect people who have been coerced and threatened, and, where necessary, we need to create safe spaces to have these conversations. At universities, you are untainted by political money from overseas. In the Chinese diaspora, we need to create or help or reinforce independent media platforms, because at the moment they are being completed drowned out. We are losing—literally losing sovereignty over the public discussion places in our countries.

Mr. LUMPKIN. In addition to losing control of the narrative, you lose the audience. You lose that audience to connect with not on just that issue but other issues.

The attention span for many people is very short. That is why social media platforms, the early—you know, 140 characters. You can captivate and actually change and influence people. But what we don't want to do is cede this space to our adversaries and lose access to the audience.

General BREEDLOVE. So, sir, I would just echo that by saying, in military terms, we have to take the field. If the only voice in the fight is that attacking our democratic institutions, then that is all that the people will hear, and we will be diminished. We have to purpose to take the field.

Mr. LAMBORN. We have talked a lot about information campaigns by the U.S. and how that is important. But sanctions in other human rights arenas has been very effective. The Russians vehemently reacted against the, if I say this correctly, the Magnitsky sanctions when that law was passed by Congress and signed by President Obama, which shows that we hit a nerve. It was effective and continues to be effective.

Do sanctions on high-placed officials in Russia and China have a place to play in this campaign that we are waging?

General BREEDLOVE. I have been outspoken on this a little bit, so let me take the first shot.

Of course our sanctions have helped, and they are effective in many ways. But if the only tool we use are sanctions and if they are always under sanctions, they become the new normal and they begin to diminish in effect. And the longer they are in effect, the

longer they have to find out ways around them, through shell companies and other things that are happening.

So that is why I advocate, as I did in my opening speech, we need a more all-of-government response. We need to look into the other silos where they are using tools against us and also open up our thoughts and imagination there.

Mr. LUMPKIN. And if I can, we are not going to message our way to—it is not a panacea. We are not going to sanction our way to get where we need. We are not going to kill our way. It is about having a layered approach in our national policies to ensure that, from a security perspective, the American people are safe.

Mr. LAMBORN. Thank you.

The CHAIRMAN. Mr. Brown.

Mr. BROWN. Thank you, Mr. Chairman.

And thank you to the panelists for being here today.

General, this question is for you. There is a saying that the best defense is a good offense. This is an adage that has been applied to many fields of endeavor, including sports and combat. I recognize that this strategic offensive principle of war might not be applicable to our nuclear defense strategy, but when it comes to our cyber strategy and our information operations, shouldn't this principle be applied? And, really, the question is, are we doing enough offensively?

I recently visited Latvia and Estonia and Ukraine, had an opportunity to speak with U.S. and partner officials, both military and nonmilitary. And I couldn't help but walk away, you know, with the perception that we are just not doing enough offensively.

Can you comment?

General BREEDLOVE. We like to say as a fighter pilot, "The best defense is your missile on the way to your enemy."

So, sir, in short, I don't think we are doing enough. We have sort of ceded the offense. We are under attack. Now, we have to take a more offensive reply, is the way I would offer it.

And it goes back to the answer I had for the other Congressman, and that is that, especially in the information space, we truly have not taken the field yet. And we don't have to disinform, but I believe there are a lot of truths about Western institutions and values that we can use in a more offensive way.

Mr. GARNAUT. Look, I might take a slightly different angle on this. I think, especially in relation to China, we underestimate the amount of defensive work we have got to do. And so I think offense is a terrific conversation, but I would first want to make sure that we have actually begun our resilient strategy at home. Because if we don't have that foundation, we can't get very far. So it is just a sequencing issue for me.

Mr. BROWN. And then let me follow up with you. Is it "Garnaut"?

Mr. GARNAUT. "Garnaut."

Mr. BROWN. Okay. Thank you. I want to follow up not on this question or your answer to this question but your response to Mr. Larsen about the Confucius Institutes. And we have one at the University of Maryland. They are basically—they are springing up all over the country and the world.

Just last month, the FBI [Federal Bureau of Investigation] director testified before the Senate Intelligence Committee that the Chi-

nese Government uses these nontraditional collectors, like the Confucius Institutes, to exploit the open research and development of the U.S. and serve as outposts—now, I am paraphrasing—of Chinese overseas intelligence networks.

You suggested that, you know, with the Confucius Institutes, as long as you know that they are there—transparency and accountability. My concern is that, number one, they are paid for by a government that has a modus operandi of influencing private-sector, nonprofit, and academic institutions to promote its policies and its objectives. And, number two, how do you police, you know, so many universities and campuses around the world?

So I guess my question is, what about a set of standards that would be applicable? And maybe even reporting? And how do you balance that particularly with Confucius Institutes on a college campus, where we invite freedom of expression?

Mr. GARNAUT. I couldn't agree more about the need for standards. There are some pretty basic standards that often get buried in the top drawer when it comes to Confucius Institutes. For example, I don't understand the need for secrecy around the contractual arrangements that are often set up. Of course, they should be transparent, they should be on the website.

I don't see why Confucius Institutes, unlike almost any other similar foreign cultural organization, needs to imbed itself in universities. So, going forward, I would encourage university administrators to keep them at arm's length.

And where we see problems with Confucius Institutes, it is almost always because universities have failed to impose, you know, even the most basic accountability. And you see the institute kind of moving or seeping into decision making elsewhere in the university. So if you tightened up management and you improved accountability, you would go a long way.

But I would just add that there has been such conversations, there has been such attention on the Confucius Institutes, I wouldn't want that to distract us from all the other stuff which is more difficult to see, we have got to work harder to see.

Mr. BROWN. Thank you.

The CHAIRMAN. Thank you.

Mr. Wittman.

Mr. WITTMAN. Thank you, Mr. Chairman.

Panelists, thank you so much for joining us today.

Mr. Garnaut, I wanted to begin with focusing on the Chinese One Belt, One Road initiative and the things that they are doing to make infrastructure investments in places like Sri Lanka, where they are developing a port there, and in Djibouti, where they built a military base.

What we are seeing is investment that is being guised as economic, that has definite strategic implications. And all you have to do is to talk about neighbors in the area. India and others feel very, very differently about the intentions of those efforts by China.

Can you give me your perspective from your—in your testimony, you said that some of these efforts are about winning without fighting, so essentially winning by other means. And that is creating strategic blocks to, I think, take away the ability for other countries to do certain things and therefore take away their capability.

And how do these types of what really are influence operations by China, how do they play into this strategy of winning without fighting? And can these activities be seen as tipping points for sites and other activities around the world that may include further expansions in these areas under the guise of economics for these particular nations?

Mr. GARNAUT. Look, I think the example of Djibouti has been instructive to all of us—and Sri Lanka. Too often we are seeing that things that were advertised as just pure economic investments in infrastructure have ended up being used in this process of debt-trap diplomacy——

Mr. WITTMAN. Yeah.

Mr. GARNAUT [continuing]. To kind of change a leasehold into freehold ownership of crucial infrastructure.

So there is a real problem there. The information is now in; it is no longer an abstract, hypothetical process. And it is much harder for developing countries to tackle this than robust democracies, because it is easier for the elite to be bought off and to actually sell out their national interests without the same degree of accountability.

So the pattern now is pretty striking. Those two examples that you mentioned—you could have mentioned a couple of others, including Pakistan—where, you know, the countries should never have signed up to that degree of debt, and it gives China enormous leverage, which it can use for strategic purposes. So, yes, we are all on notice that this is a problem.

Mr. WITTMAN. Very good. Thank you, Mr. Garnaut.

General Breedlove, the United States military, I think, has made a lot of advances along the lines of cyber issues, establishing some centers for excellence, especially the NATO Cyber Center for Excellence. And Estonia has been a great example about how those things have progressed. And, obviously, your time there with NATO and with EUCOM, you know, was a great part of that.

But it seems like, though, on many of the other less-definitive issues, the U.S. is lagging behind somewhat. And I wanted to get your take on what are the necessary steps going forward for the U.S. to do more to protect its data, and not just data in a defense system but also data on the commercial side; to safeguard the American system from dirty money, that money that kind of makes its way through and undermines efforts for us to guard information and to keep a strategic superiority place for us; and, also, to restrict the influence that nations like China are having over our universities?

Mr. Garnaut spoke a little bit about these Confucius Institutes, but it is more than just the Confucius Institutes. That is one element of it, but there is a lot of other, more clandestine efforts that are going on there to have influence but also to gain intellectual capacity back to China.

So I wanted to get your perspective there on those issues.

General BREEDLOVE. Thanks for the question, sir.

And I would just disqualify myself about talking about the dirty money. I think that the answer there is what we have talked about a couple of times: transparency in business practices and standards. And that is about as far as I can go on the economic front.

I think you really hit the nail on the head when you mentioned the exfil [exfiltration] of commercial data. One of our past DNIs [Directors of National Intelligence] said that we have had terabytes—terabytes—of proprietary data about our most advanced systems that have been exfil'ed from our commercial entities.

And so I think we need to recognize that that is a strategic problem for the United States, to include its military. And then we probably need to rally around those who are struggling. And I think, in general, we look to our commercial entities to do it on their own. And so I would advocate for sort of increased collusion on how we defend these very important and valuable things.

And on the restricting influence on universities, again, we run up against those things we value, which are freedoms of expression and so forth. But I think Mr. Garnaut hit it right on the head: Having some standards and setting expectations before is really important. And that then empowers the universities to not be seen as an ogre in the business, and they can adhere to those standards and expectations.

Mr. WITTMAN. Very good.

Thank you, Mr. Chairman. I yield back.

The CHAIRMAN. Mr. Panetta.

Mr. PANETTA. Thank you, Mr. Chairman.

Gentlemen, good morning. Thank you for being here.

Mr. Garnaut, kind of going a little bit more into what you were just talking about, I realize that we have talked a lot about our country's offensive and defensive capabilities. Talk to me about other countries' offensive capabilities and our coordination with those other countries, if you can. How is that? How are we at that point?

Mr. GARNAUT. Well, we are not. So this is the very early stages of a long, long conversation.

So the answer is that, you know, it only seems like yesterday we were all woken up to the defensive piece. And I think there are many countries, you know, in this game that are actually actively working out the offensive piece, let alone coordinating between each other.

So the answer is it is all to be done.

Mr. PANETTA. Please.

General BREEDLOVE. I would just point out some exercise experience, not real-world experience.

In an alliance with multiple nations, each nation brings different levels of restrictions to its use of offensive power. And sometimes in these scenarios, again, in exercises, we find that while one government will not approve something, another might use their tool. And so commanders, who have to deal with alliances, have to understand the ability to do bilateral work inside of an alliance to use tools that may not come to the front.

And I would just say one more time, a third time: In exercises we have looked at this.

Mr. PANETTA. Understood.

Mr. LUMPKIN. And I do have one real-world example of where this coordination has happened, and that is the counter-ISIS mission among the coalition.

The messaging piece—there was a strategic communications messaging group that worked hand-in-glove together because of authorities of different countries' understanding of specific audiences, where we could synchronize and coordinate the messaging to make sure we hit the right message to the right audience at the right time with voices that would resonate.

Mr. GARNAUT. Let me stand corrected. On ISIS, that is right. There is a lot of work to be doing in actually emulating the work we have already done on ISIS, including working together.

Mr. PANETTA. But it appears that all of you would agree that, when it comes to these revisionist countries and their guerilla geopolitics, there is not really a coordination amongst the other nations in pushing back on them.

General BREEDLOVE. NATO is beginning to have those conversations.

Mr. PANETTA. Great.

General BREEDLOVE. I have been out of NATO for a little while now, so I can't speak for their most recent conversations.

Mr. PANETTA. Great. Great.

Thank you, gentlemen.

I yield back. Thank you, Mr. Chairman.

The CHAIRMAN. Mr. Coffman.

Mr. COFFMAN. Thank you, Mr. Chairman.

In U.S. campaign finance laws, we have provisions whereby if someone wants to do political ads on radio or TV, they have to disclose who they are, who the organization is. We have never updated those laws to reflect social media platforms. Do you think that that transparency would serve the American people well?

I am wondering if you all might comment on that, starting with you, General.

General BREEDLOVE. Absolutely. It is a really short answer. But, clearly, we did not understand what has happened in our past in this, and we need to be a lot better at it in the future.

Mr. COFFMAN. Thank you.

Mr. LUMPKIN. I think there is something "there" there with that. But I also think that there should be some sort of credibility rating on the veracity, not just who is paying for it, but is it true, is it not true. And I don't know if it is—you know, historically, you get five stars because your truth over time for 20 years is, you know, at the top 1 percent, or however it works. But I think we need some sort of veracity scale to see that what is actually coming out is true and accurate.

Mr. GARNAUT. And if I could add, on China, so China doesn't yet work the English language social media in the same way that Russia does. Maybe it is learning; maybe this is all to come.

But where we've really got a problem is in the Chinese-language social media systems and channels. So the fact that China has been successfully able to block out the big American platforms—the Facebooks, the Twitters, et cetera—has given it a near monopoly of Chinese-language social media, and it follows the diaspora abroad.

And so we have actually lost—you know, these messages that are going to most Chinese-language social media users in Australia and the United States are filtered through Beijing, so we have ac-

tually lost the delivery mechanism. So it is well beyond just tagging that there is some government involvement in the message; it is filtered and delivered and created by a Beijing-sponsored platform.

Mr. COFFMAN. Thank you.

General Breedlove, as a former U.S. commander for European Command, you had mentioned in recent testimony—in prior testimony about the Russian attack against its former spy and his daughter as not necessarily an act of war but a warlike act.

In Article V of the NATO charter, it speaks to the requirement for NATO members to come to the defense of any NATO member who has been attacked. The problem is what constitutes an attack.

And what the Russians—I almost said "Soviets." I don't know if there is a difference. But what the Russians have been developing is these hybrid tactics. And so, you know, it is about, you know, information operations. It is about using covert forces in conjunction or to augment indigenous elements that they have stirred up within the country. They have obviously done this in the Ukraine. My guess is they could very well be looking at the Baltic States as a test to break NATO.

How well-defined is Article V? And what would you anticipate a European response, a NATO response in something that may not be a clear-cut conventional attack?

General BREEDLOVE. Congressman, this is a tough question that is being discussed in NATO when I left and still is being discussed.

When do these—and I liked—I used that, "hybrid," in my own testimony. I really like Gerasimov's words because they illustrate what you are talking about: active measures and asymmetric methods.

But Article III, defense starts at home. Article IV, we consult with our allies to determine have we been attacked and what is the response. And Article V is then the collective response.

So that process kind of walks through. And at the point that we are now, most of the nations are using that process individually to determine, have we had an Article V sort of response. And so it is hard to draw the line of what is and what isn't.

And, frankly, I believe Mr. Gerasimov and Mr. Putin believe they can get away with different things in different countries, to include our own. They have a line which they think they can operate to.

And so it is a tough question to answer, and I can't give you a definitive piece.

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

The CHAIRMAN. Mr. Garamendi.

Mr. GARAMENDI. Thank you, Mr. Chairman, and thank you for this hearing. In my view, this is an extremely important hearing, and it is one of a series that I believe we ought to engage in.

I recall a hearing in the Senate, about a month ago now, in which the heads of the intelligence agencies, when dealing with this asymmetric warfare, said that it appeared to them that there is no risk to Mr. Putin; there has been no pushback.

Last week, the Departments of Energy and Homeland Security issued a bulletin that clearly said that Russia had hacked into our electric grid systems, into our power plants, including nuclear power plants, and various transportation, including airports, and

that they had probably gained control of those systems. In other words, they could shut down the electric grid; they could shut down the cooling systems in power plants, probably including nuclear power plants.

The question that this committee must ask Cyber Command, who is responsible, as I understand it, for the defense of this Nation against cyberattack—and, by the way, the Departments both said it was an act of war.

The question for this committee is to ask the question of Cyber Command: Are you defending the Nation? And what can you do to make Russia understand that there is a risk, that they will pay the price for what they have already done and what they might do in the future?

So, Mr. Chairman, this is more to you, to ask you to have Cyber Command in here. I understand they may be here on April 11. And we must ask them the tough question: Are you defending this Nation? If so, how did it happen—how did it happen that the Russians are able to gain control of our key infrastructure? Which would be a pretty good indication that our Nation is not being defended.

And, furthermore, what instructions has Cyber Command or any government agency been given by the President to defend this Nation and to strike back? If there is no risk, then we are at serious—if there is no risk to Russia, then we are at serious risk.

This being the Armed Services Committee, Mr. Chairman, our task is to hold this administration accountable, to find out what they are doing to protect us or what they have not done and what they could do. And until we do that, it is very clear, from the ongoing information war and cyber war, that there is no risk to Russia for what they have already done, which has been described by our Homeland Security and the Department of Energy as an act of war.

Mr. Chairman, we have a job to do here, because this administration is not doing it.

If any of you gentlemen would like to comment, please do. You have 53 seconds.

General BREEDLOVE. I would just add that, when we consider giving Mr. Putin risk, we certainly need to, as you have talked about, look in the cyber and information spaces, but as I have said already this morning, we need to also look in the other spaces. We need an all-of-government reply in these areas.

Mr. GARAMENDI. If I might, sir, in your initial testimony, you said that we needed a plan, a comprehensive plan. We don't have one, obviously. I would be delighted to hear your idea of what that might be. And, obviously, you won't do it in 16 seconds, but you are welcome to come back to my office or maybe to another hearing.

The CHAIRMAN. Mrs. Hartzler.

Mrs. HARTZLER. Thank you, Mr. Chairman.

And thank you, gentlemen, for this very, very important hearing.

General Breedlove, it is good to see you again. I am used to seeing you in uniform, but I appreciate your expertise continued and your testimony.

And I just want to highlight a few things and then bring it home and then ask for your advice.

You say that Russia's interference in the election is merely a symptom of the larger hybrid war against the West in which economic, cyber, and disinformation tactics are used in conjunction with conventional forces in order to exert force, pressure on the adversary.

The American people need to know this, and I am so glad we are having this hearing today.

You go on and say: Waging a conventional war against the West would be unfavorable to Russia. As such, it has used hybrid warfare to break up Western unity. Exploiting divisions in the U.S. society and promoting a cultural war is one key element of Moscow's effort to weaken the West.

That is spot-on.

I want to bring it home. I represent part of Missouri, and I represent the University of Missouri. That is my alma mater. Here are a couple of headlines that came in my local paper there.

"Report: Russia sparked fear at the University of Missouri during 2015 protests."

Another article: "Mueller indicts Russian agency cited as origin of University of Missouri disruption efforts." We had some unfortunate protests, some discord locally on our campus, and the same people that were involved in the Presidential election from Russia inserted themselves into our local issue to make the matter worse.

And there was a really great report done by Lieutenant Colonel Jared Prier, who did the research and connected the dots and brought this to light. I just want to read a couple things that he said.

He said, "Defendants, posing as U.S. persons and creating false U.S. personas, operated social media pages and groups designed to attract U.S. audiences. These groups and pages, which address divisive U.S. political and social issues, falsely claim to be controlled by U.S. activists when, in fact, they were controlled by the defendants."

He goes on and says, "The role of the Russian trolls and bots wasn't to generate a controversy but to feed and amplify it in an attempt to fan discord."

And then he had another real quote. He says, "It is like when someone gets in a fight and there is someone in the back of the room saying, 'Yeah, punch him. He'll think you're weak,' egging it on."

And so we have got to bring this to light. And I think, as Americans, it is time that we rally as a family. You know, it reminds me, back home in Missouri we have a lot of common sense. And sometimes we have our own interfamily squabbles, and the brothers and sisters may fight a little bit. But, boy, the neighbor kid or somebody else wants to attack our brother or sister? Boy, we rally around that family, and don't mess with my family.

And I think, as Americans, we need to wake up. This is what our adversaries are doing across the world, whether it be Russia or China. They are exploiting our own family squabbles, making them worse, making us not only fight ourselves but fight other people and weaken the whole thing. And it is time that we wake up to this.

And you conclude by saying we need to take a position, establish policy and execute it. And all of you have given a lot of good advice. And I know we need a strategy.

But I wanted to ask you General Breedlove, specifically on this issue, where you have social media from the Russians coming in, interfering with our own family squabbles, what do you think our policy should be? And what should the execution of that be? What should we do in retaliation for them interfering?

General BREEDLOVE. So, very quickly, to pile on, I use this very example as I speak around the country of what happened at Mizzou. And it was even multilayered. After they instigated problems, they went back in and chastised the local press for not covering their disinformation and further spreading it. It was really audacious, what they characterized there.

The first thing, ma'am, is that America needs to understand this. There are other examples equally as bad as Mizzou surrounding removing Confederate statues, both sides being egged on by the Russians. In order to try to keep oil prices down, they are instigating fights on both sides of things like oil pipelines and fracking in order to cause discord and disharmony and to hopefully continue to suppress those efforts to keep oil prices up.

And so the first step, I think, is making Americans aware that the Russians and the troll factory there in Saint Petersburg, the Internet Research Agency, is out there orchestrating these battles in these spaces, and make our folks aware that when they go into their social media they are getting an echo chamber of their own thoughts. They are really not seeing both sides. And in that echo chamber they are being fed by these people who are trying to incite, again, on both sides of the issues.

So awareness first. And then to begin to hold responsible those—and I think we need to start having tough conversations with those that prepare the social media platforms on what they allow in their spaces.

Mrs. HARTZLER. Thank you.

The CHAIRMAN. Mr. O'Halleran.

Mr. O'HALLERAN. Thank you, Mr. Chairman.

I guess I am going to make some statements and take up some time. But I am an old investigator here, and I look for verification of issues and gaps in issues. And we are dealing right now with an issue that, if they attack our electrical grid, we could find some ways of changing the process, but they are shaping our citizens' minds. They are shaping the values of how people feel about our government and our country. And that is something that we just don't turn off. That is something that we have to gain back the trust of the American people and be able to do that.

And it is not just social media. I listen to TV also. And it is "I think," "I believe." There is no verification of anything anymore.

And I have heard statements of whole-of-government approach all year long, and I don't see it where it is working. And I heard it earlier today. This is the kind of stuff that started after 9/11. So we have been 17 years of talking about whole-of-government, and it is apparently not working.

It is hard for me to believe—I was channel surfing one time, and I saw RT on. And it took me about 5 minutes to understand what it was about. And I didn't even know at the time it meant Russia.

And now here we are today, and I cannot believe that our intelligence people have not picked up on this for the last number of years. And so they either missed what was happening totally, they chose not to make it a priority, or they did not understand the consequences. Because if they knew that this was occurring and they didn't take the appropriate action over the last 17 years, then we really have a problem. We are behind by 17 years. And I believe all of you made that type of a statement.

And, Mr. Lumpkin, you said you were scratching your head right now, and you also said that the world has changed. And I am shaking—and silos are still there after 17 years. I find it very difficult to—if I were sitting at home as an American citizen listening to this, I would be not only shaking my head but I would have to question the viability of how our government addresses these serious issues on an ongoing basis.

I am new in Congress, but I have to tell you that, like many American citizens, I want to be able to believe my country is going to react in the appropriate way when this occurs, and I haven't seen that at all, whether it is this hearing or subjects leading up to this hearing, where the faith of the American people, in making sure that they trust their government and trust what they are hearing across the entire spectrum.

We talked about standards here today. It appears that, in my lifetime, standards have not only gone down because of social media, but also because of ratings and the fact that we don't have much investigative reporting anymore and it is all quick, 30-second sound bites or 3-minute sound bites and move on to the next issue.

So having given—I have a little bit of time here, so what do you think?

General BREEDLOVE. I will be really quick, sir.

I think that after 9/11 we did have sort of an all-of-government response, but it is my opinion that we are extremely limited in our all-of-government response on issues since then. We tend to take very military approaches to Middle Eastern problems, and we tend to take very economic approaches to Russian problems.

Mr. O'HALLERAN. Anybody else?

Mr. GARNAUT. If I could just add, essentially we are talking about intangible harm, and it is very intrinsically hard to define and to see, so where there is no body bags, there are no explosions. So it is easy to be disillusioned on where we are.

But 18 months ago, we weren't even talking about this problem. At least there is now a conversation. These——

Mr. O'HALLERAN. I am going to interrupt you because my time is running out.

Mr. GARNAUT. Please.

Mr. O'HALLERAN. That is the problem. We weren't talking about it.

Mr. GARNAUT. That is right.

Mr. O'HALLERAN. But I guarantee you we knew about it, and we weren't working at it. And I guarantee you, because we knew about it, we should have been working on it.

And the issue of transparency, we have talked about a lot today. We haven't defined what transparency means. We have said the word, but we really don't know what that means.

And I yield. Thank you.

The CHAIRMAN. Mr. Scott.

Mr. SCOTT. Thank you, Mr. Chairman.

I would like to follow up a little bit on what Mr. O'Halleran was talking about.

When Tom Brokaw was on the news, he was not only the anchor, but he was the managing editor of his news show. And I do not believe that Tom Brokaw would have told America a boldfaced lie. Today, it seems that we don't have anchors who are also the editors but that the people that are on TV are simply repeating what is on a Teleprompter, what their editors are telling them to say. And while I think it is worse on the television, I think that is also accurate in what happens in the print media today.

And so, General Breedlove, you mentioned in your testimony, "Russia took full advantage of this new media landscape."

And when we are talking about the weaponization of information, information can either be true or information can be false. Would it be more accurate to say that it is the weaponization of misinformation?

General BREEDLOVE. Yes, sir.

Mr. SCOTT. And then, as you spoke, Mr. Garnaut—is that right?

Mr. GARNAUT. "Garnaut."

Mr. SCOTT. You spoke about how transparency goes a long way to solving the problem. And what transparency would do is let the American public know what is true and what is false. And if it is false, then hopefully it would not have the influence on our beliefs that it would have if it was true.

Mr. GARNAUT. Look, just as a former journalist, let me defend journalism for a second here. And that is to point out, in Australia it has been a handful of journalists who have really pushed the issue of foreign interference to the front of the agenda. So, over several years, some hard investigative work has been done to actually illustrate the problem, put it on the front pages, and start to define the harm and to show the state connections.

So media still does have a role——

Mr. SCOTT. That may be happening in your country, but in America a news outlet is either pro-Obama/anti-Trump or anti-Trump/pro-Obama. I mean, that is——

Mr. GARNAUT. That sounds tricky.

Mr. SCOTT. It is just the way—it is unfortunate. But most news outlets in the U.S., if we can call them news—I think "media" is a better way to portray them now, because I don't consider them to be news anymore—give just enough truth in their story to lead people to jump to the conclusion that they want the people to jump to, which creates the chaos.

So I am very much in favor of journalism. It is the editorialism that I think is destroying the credibility that our news outlets have with America.

And if I could, I will quote you from a Pew Research poll. And Pew does pretty good polling. 2017, this is just over a year ago, Republicans—"Percent of U.S. adults who trust the information they

get from national news organizations: Republicans, 11 percent." That means that 89 percent of Republicans don't trust the national news. "Democrats, 34 percent." That means 66 percent of Democrats don't trust the national news. And 15 percent of independents trust, so 85 percent of independents don't trust the news outlets.

And I would just tell you, I think the loss of journalism has been one of the real problems in this country, and the bias that is out there. But if it is not the truth, then it is propaganda. And as we have seen in Missouri, I think this is going to get worse, if the journalists are not allowed to tell the truth.

Which brings me to you, Mr. Lumpkin. You talked about we have the information but what we don't have is a conductor. And shouldn't the journalists be the conductors? Shouldn't the journalists be allowed? What is your thought on the conductor?

Mr. LUMPKIN. You said something at the front end of your statement here, is that if it is not truth, it is propaganda. I wish it was that easy, from where I sit, and maybe it is just from where I was sitting, is that, for example, this to some person is a receptacle; other person, it is a bottle of water; somebody else, it is a hydration device.

I mean, that, in conjunction with five different pieces of information, or different stories altogether, can shape somebody's mental picture of a situation.

And that is where, I think, the key is. You have to understand your audience and what resonates with them and what doesn't resonate with them. For example, at the GEC, there were some messages that worked really well in a small village in Libya that would have no take in Malaysia. Same message, but culturally they look at the world differently.

So messages and information and truth are kind of—they are not an absolute. Because all of those things I just mentioned about this bottle of water are true. I mean, it just depends on what is your perspective and how you look at it.

And I think that the key is that you have to understand the audience you are trying to hit. You need to devise messaging strategies that will resonate with that audience. And then you have to have a data feedback loop. Did it hit? Did it take? Did it move the needle on behavior?

And behavior change is the one of the hardest things to measure, especially in a short period of time. But you have to have—it is about data to make sure that you are managing the process and the information.

The CHAIRMAN. Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

And I want to thank our panel of witnesses for your testimony today. And, in particular, General Breedlove and Secretary Lumpkin, thank you both for your service, as well, to the Nation.

So, Mr. Lumpkin, if I could start with you, I am a big fan, as you know, of the Global Engagement Center, and I believe that it really does have a critical role to play when it comes to countering messages perpetuated by our adversaries.

And I know we have talked about the Global Engagement Center several times here today, and while I am glad that the State Department has finally accepted the allocated transfer of funds from

the Department of Defense to assist in the effort, of course pending congressional approval, I am still worried that it is not being utilized to its greatest potential and that there now exists a lack of leadership guiding it toward success.

I know that we have to make better use of the Global Engagement Center and we have to figure out how we can better support its mission. But, domestically, there is no department or agency of the U.S. Government tasked specifically with protecting the U.S. public from foreign propaganda, and, of course, probably rightly so, since we have to be mindful of First Amendment protections and such. But there is, again, no U.S. public—no one protecting the U.S. from public or from foreign propaganda or various forms of information warfare.

What role do you feel that industry has to play here, and what are their responsibilities?

Mr. LUMPKIN. I think that industry does have a role. Again, I kind of mentioned earlier a—again, I would love to see some sort of veracity scale on what is going out, based on historic trends, of whether a news piece or that source is reliable or not. That is something that could be done by industry.

But because of the diverse nature of media in this country, whether it is social media, print media, word of mouth, blogs, it is very, very difficult to control while protecting privacy of the American people as well as those First Amendment protections that we have. So, extremely complicated.

But I do think we are at the point where we need to have some serious discussions about the best way to preserve those freedoms of Americans but at the same time make sure they are getting effective and accurate news.

Mr. LANGEVIN. So, Twitter announced that they are looking to partner with outside experts to improve what they describe as the health of their content, with the underlying goal of, among other things, cutting down on abuse and manipulation of the platform.

This is on top of several other steps that have been taken to date, which include, from what I understand, their new initiative to increase transparency of political advertisements prior to the elections this fall. Much work of course remains to be done still, I believe, but I am encouraged that this is a positive step in the right direction.

But how could the government work to better assist companies like Twitter to identify threats from foreign state actors who are seeking to engage in information operations against the United States?

I will start with Secretary Lumpkin, but if our other two panelists want to chime in as well, I would appreciate it.

Mr. LUMPKIN. I think the first step is have the dialogue, I mean, because you have to understand the privacy restrictions and privacy goals that each of these social media platforms, for example, have with their clients.

Mr. LANGEVIN. I think the dialogue is important, but it has to, I think, go beyond that.

Mr. LUMPKIN. Yeah, no, but I think—when I got to the GEC, we had virtually no relationship with some of these social media platforms about understanding how they saw the world. I think that

we can work with them. In fact, if you see some of the things that the private sector has done to regulate content, whether it is people screening the content or removing the hundreds of thousands of Twitter handles that have been removed by Twitter, they are doing things. We just have to make sure that we are working with them and not against them. Again, I think it is just about opening the dialogue at this point.

Mr. LANGEVIN. Okay.

Anybody else want to chime in?

General BREEDLOVE. I would just add, I agree. And I think that part of that conversation with these providers is what is their intent, what do they see as their responsibility. They are taking actions, but those actions are in sort of limited ways. And is it their intent to try to begin to ensure the veracity of data or content, that would be a good conversation.

Mr. LANGEVIN. Thank you.

Thank you, Mr. Chairman.

I would just say this is really a challenging problem, because this is a nation-state attack, and they are using our own private companies to carry out those attacks. And they are not necessarily the ones that are equipped with being able to defend against such a nation-state attack, with all the tools of statecraft and power that can be brought to bear. And this is a difficult challenge and dilemma that we have to tackle.

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

The CHAIRMAN. Thank you.

Dr. Wenstrup.

Dr. WENSTRUP. Thank you, Mr. Chairman.

Thank you all for being here.

This has been an interesting conversation today, to say the least. I would like to compliment Mr. O'Halleran on some of the things that he had to say today. But it seems to me that our own people sometimes don't know what we have until it is gone. And today we have an adversary that is a very patient warrior in all that they are doing.

And I found it interesting—I appreciated Mr. Garamendi's passionate response to the situation today, but, in my opinion, he just played into exactly what they want us to do.

And I look at the election cycle. For the Russians, it was heads, I win, tails, you lose. If Hillary Clinton wins, we have destabilized her and criticized her, and if Donald Trump wins, then he is not legitimate. They got it coming and going, either way.

And then he took this issue today—and he is a friend. I appreciate his passion. But he turned it into "this administration," as though this problem just started in January of 2017. And let's not forget, Mitt Romney said Russia is our biggest geopolitical foe, and he was laughed at. Adam Schiff has said the Obama administration response to what was going on was inadequate.

We have to move forward here, folks. Because that type of thing, blaming the other administrations or whatever, is not going to get us where we need to be today. And that is exactly what they want us to be doing.

And we do need a whole-of-government, Republican and Democrat, to go after this issue and bring it more to the forefront and

America's awareness. Because, you know, we always judge a country by how many want in and how many want out. And America has usually been the place where people want in, to become Americans. Now we have them wanting to come in to disrupt America. And I am curious if we are really even looking at that.

But my concern is, you talked about the new normal, sanctions would just become the new normal. And my concern is their way of life, for Russia and China, perceived as the new standard in the world. My question to you is, how does this affect our democratic institutions and our rule of law and what we consider international norms if they become the standard bearer of what is supposed to be normal, as opposed to democracy?

Mr. GARNAUT. Can I just comment on the importance of something you raised there? And that is, I think in Australia we have made some progress in this respect: the importance of establishing a consensus about the nature of the problem and the principles that inform and underpin your response.

And so, one, democracy is under attack. You know, that is the core of our systems, our sovereignty. Two, we will defend it against interference from all comers, whether it is Russia, or China, or Iran, or ISIS.

And once you have established, you know, a firm consensus, then you can start building your resilience strategy. But until you have your consensus, you are just groping in the dark and it is all over the place.

Dr. WENSTRUP. Thank you.

Any other comments?

Mr. LUMPKIN. I do.

I know the name we usually use for this is "hybrid warfare." I prefer the term "modern warfare," because this is what we are looking at. This is not just, you know, a slice in time; this is what we are looking at in a hyperconnected world. So we have to develop strategies that are layered, comprehensive, that transcend elections, that do all of these things to protect, again, our national security and the American people.

But this is not going away. As social media and new media platforms iterate, we are going to see this morph, shift, and change. And we can either be chasing our adversaries—I would like to catch up with them now, let alone surpass them. But we need to put some more effort here.

Dr. WENSTRUP. General.

General BREEDLOVE. Just very quickly, I am in violent agreement with the last couple of things you said. It is really about them attacking Western institutions, democratic values, democratic nations.

And as was said in a couple of responses, they are in on both sides in a lot of these, because it is not really about one side or the other winning. It is about causing disarray and loss of confidence in the things that our citizens need to be confident in.

Dr. WENSTRUP. Thank you.

I yield back.

The CHAIRMAN. Ms. Gabbard.

Ms. GABBARD. Thank you, Mr. Chairman.

Thank you, gentlemen.

General Breedlove, you talked about, in your opening remarks, a few examples of American interference in foreign elections in the past. To add to the examples that you gave, there was a study that was released at the end of 2016 documenting 81 elections in 47 countries between 1946 and the year 2000 where the United States either overtly or covertly sought to influence the outcome of elections in these countries and were successful more often than not. And this doesn't include any of the CIA or military regime-change overthrows that also happened in addition to this.

So, you know, as recent as the Iraq war—during the Iraq war, we paid millions of dollars to plant propaganda articles in Iraqi newspapers; sought to influence Russia's elections in 1996.

I say all this to raise the question about, if someone turns on cable news today, and to hear a lot of the conversations here, one would think that Russia's actions in 2016, this is the first time this has ever happened, and that the United States does not have the history that we do with the tactics that we have and may continue to use.

So my question is, how should anyone take the issues that you are raising and the attacks that you are citing in any context other than the historical context that exists?

General BREEDLOVE. So, ma'am, you made the point that I was trying to make in my opening statement, that I am not surprised and I don't think anyone in America should be surprised that Russia tried to influence our election, because, as you have aptly described, we have been into that business in the past.

And I would like to join Mr. Lumpkin's remarks, in that this word "hybrid war" I don't think gets it. It makes it sound new and exciting, and it is really old tools used in new ways.

And what I didn't say well in my opening statement is the thing that surprises me the most is the boldness that Russia believes it can have in our spaces, that they can do these things and absolutely get away with them.

Ms. GABBARD. Have we lacked that boldness in U.S. actions in other countries?

General BREEDLOVE. As I said, I am trying to open the conversation——

Ms. GABBARD. Sure.

General BREEDLOVE [continuing]. Beyond the election, to all of the elements of national power: targeted assassinations, SCADA [supervisory control and data acquisition] attacks, information attacks, elections.

So I guess what I am trying to say is there is a broader attack on us than just the election piece. And we need to be examining that in a holistic view and then, again, I think, replying in a holistic way.

Ms. GABBARD. Thank you.

You know, Mr. Garnaut, you talked a lot—obviously, you focused a lot on China, on China's actions, both in Australia but generally, and in different ways that they are seeking to influence policies, elections, views, et cetera.

Why—and, you know, whether it is you or General—and any of you who would like to answer this—why is it that, again, all we hear about is Russia's actions generally if you turn on the news,

whereas there are countries like China, like Saudi Arabia, like Qatar, and other countries who, you know, purchase TV ads, who fund think tanks here in Washington, who, you know, who fund institutions in our universities, seeking to achieve that same objective? Why is it that Russia's actions stand out from all of the rest that have been going on for quite some time?

Mr. GARNAUT. That is a great question. And I think one answer may be that because China is very good at it. They put an enormous amount of effort into making sure we don't talk about what it is doing. So if you look at the pattern of influence and interference, a lot of it is about suppressing contrary voices in our systems, you know, shutting down conversations about the nature of the Chinese Communist Party and what it is doing, while nurturing others.

And it is quite—and unlike Russia, where Russia seems to be, you know, as much for a good time rather than a long time, the Chinese are strategic and patient and they set down foundations of organizations, very consistent narratives over a long period of time, so often it is quite incremental in the way that China behaves, whereas Russia tends to do these kind of focused, sharp kind of strikes. So very different methodologies.

But you could argue that—but it doesn't mean that China is less important. You know, I think that we just failed to recognize a lot of what activity has been going on, and that needs to change and it is starting to change, certainly in Australia, and starting to change in the United States.

Ms. GABBARD. Thank you.

The CHAIRMAN. Mr. Byrne.

Mr. BYRNE. Thank you, Mr. Chairman.

Gentlemen, yesterday, China approved a new broadcasting entity called Voice of China, which, obviously, is mimicking the Voice of America. And they are doing that to strengthen the Chinese Communist Party's ability to shape public opinion and to project a certain positive image around the world.

Do you see this as a tool for China to use to gain influence globally? Are you concerned by it? If you are concerned by it, what should we be doing about it? I know it is pretty new, but it is something we ought to talk about.

Mr. GARNAUT. Can I just jump in quickly? So we are talking there about an overt propaganda platform. So in the kind of the tricolor spectrum, the black, the gray, the white, this is white.

Now, on its own, I think propaganda is not the main focus of our concerns, but when it becomes a problem is when it is mixed with covert and deceptive work to spread. You know, the channels of distribution are really important. So rather than worry about the contents so much, is how is it penetrating our societies, and then I think you will find a lot of the black and the gray operations that we should be focused on, if that makes some sense.

Mr. BYRNE. Do the other two gentlemen want to comment on that?

General BREEDLOVE. No.

Mr. BYRNE. One of the things that some of us who have traveled to China, and certainly are trying to watch it, are observing is that a country that heretofore had been holding itself back is now be-

coming extremely aggressive. Certainly, there is some tie between that and the recent decision by the Chinese Congress to give unlimited tenure to President Xi Jinping.

Should we expect for him and for the Chinese Communist Party to further these activities to use propaganda, whether it is white, gray or black, around the world and particularly here in the United States?

Mr. GARNAUT. Well, the short answer is yes. We have seen a massive intensification of Chinese covert and deceptive operations, and that has been led by Xi Jinping, so we are in a new era. You know, I think that this pattern has become—has been becoming increasingly clear since probably the tail end of 2013. So this is a 4- or 5-year process. And I can't see any reason why that process of intensification won't continue perhaps for the duration of his tenure, which might be a very long time.

Mr. BYRNE. There has been some discussion already today about the Confucius Institutes. In some places, they are providing some more cultural information on college campuses. They have at least a quasi-legitimate role to do that, along with other countries that do that.

How do we know when the Confucius Institutes go from a legitimate activity to something that is illegitimate? And when we know about it, what do we do about it, in a democracy with rights to free speech, free association, like the United States?

Mr. GARNAUT. Look, I think when we see examples of behavior in the black, of shutting down free speech, then we actually have to be really, really tough. And if it is a pattern, then we should hold the system responsible. At the moment, I think up until now, it has been a very permissive environment. We haven't tracked how the responsibility—Confucius Institutes and other foreign-funded institutions have been used to stifle debates elsewhere in the universities. I think we have got to be much tougher when we catch it.

Mr. BYRNE. Well, I would just say, Mr. Chairman, I know there has been a lot of talk in America the last year or so about Russia and what Russia is trying to do to influence things in the United States and interfere with the operation of our society and our government, but I would say that I am equally concerned about activities from China. And I hope that in some of our politically driven attention to what Russia is doing, which is valid that we should pay attention to that, that we don't lose sight of similar and, I would say, equal activities on behalf of China to try to influence and disrupt American life and our American political institutions.

And so I appreciate all three of you and your perspectives on this. Hopefully, we will continue to study this. And I yield back.

The CHAIRMAN. Dr. Abraham.

Dr. ABRAHAM. Thank you, Mr. Chairman.

I think we all agree that this hybrid or modern warfare or whatever we want to call it, is certainly not a new concept. I would think that the Canaanites would consider the trumpets that Joshua and the Israelites blew as hybrid warfare in their time. And I would postulate that in a few years, with quantum computing and the super computers that I am told China now has the fastest of, the discussion we are having today about the hardware, the fiber

optics that are being used, will be obsolete, and we will be talking about a completely different set of dynamics and metrics as to how to combat this.

You know, I will take exception to some things that have been said about the President and the present administration being asleep at the wheel. I think this President has, for the very good thing, been able to call out what we call fake news, whether it is domestically or foreign, and this highlights where we have gone as a country, unfortunately, as to looking at how we receive misinformation or truthful information.

Secretary Lumpkin, to your statement that that bottle of water will be perceived differently from Malaysia, Syria, wherever you want to go, but, in fact, of all the things it may be, it may be a receptacle, it may be this, it is still to—it is still at least a bottle of water to everyone when it is front and center. So that—and I agree with you and to your statement.

Mr. Garnaut, I also agree with you that, certainly, some in our media have been co-opted by some nefarious governments, either state or non-state actors. Unfortunately, I don't see that changing, unfortunately. I totally agree that we need transparency in our government. We certainly have, I think, that, and we certainly need it more in the foreign fields, in the foreign actors to—I don't think that is going to happen either, unfortunately. But we have got space wars that are fixing to happen. We have things that will start occurring that we couldn't even think of 15 years ago, probably 10 years ago.

So I guess my question is, in my 2½ minutes left, we in the United States, we welcome, we actually encourage foreign development, foreign investments in our products. We have companies that are now owned by China and other foreign governments that have knowledge and they have direct access to some of our most technologically advanced equipment.

So my question to each of you, quickly, can you give me concrete examples of where this commercialization of foreign investment has directly hurt us in the national security level?

General, I will start with you.

General BREEDLOVE. Sir, so I alluded earlier to what I think is the real issue, and that is not through legitimate means, as you have talked about owning, but the exfil of commercial proprietary data around our most important systems. That is what worries me the most.

I do have a little more confidence in committees, in DOD and others, like the LO/CLO [Low Observable/Counter-Low Observable] committee that protects our secrets. And I think it is a fairly sophisticated system. I am worried about what you said, but I am much more worried about the illegitimate exfil of data.

Dr. ABRAHAM. Mr. Garnaut.

Mr. GARNAUT. Just briefly, I think we have underestimated the level of sophistication and organization of a lot of foreign-sponsored technology transfer programs. It is—so cyber is obviously a big part of it, but also the networks of scientists, how they link back up with foreign governments. We just haven't had our eyes on the ball. And I know that Congress and other institutions in the United States are now kind of more alert to the upstream technology com-

panies being sort of purchased by state-driven actors. So I am confident that there is at least movement in the right direction in this field.

Dr. ABRAHAM. Mr. Secretary.

Mr. LUMPKIN. I have nothing to add. Thank you.

Dr. ABRAHAM. Okay. And the only thing I will add in my last few seconds is that, General, I agree with you that, you know, a lot of these things are intangible, at least in conceptual ability. I hope as a Nation we can unite against this. Unfortunately, unless there is physical damage and physical, you know, human life at stake, I just, unfortunately, don't see that happening, and that is very unfortunate.

And I yield back, Mr. Chairman.

The CHAIRMAN. Mr. Bacon.

Mr. BACON. Thank you.

Thank you, gentlemen, for being here. And I have got to say for the record that it was an honor to serve under General Breedlove's command, one of the finest bosses, commanders, leaders I have ever met. And so it is great to see you back here today, sir.

It is clear to me that we are under attack in a different way, and we have to be clear with our citizens with that. It is imperative that we not make this a partisan matter. This should be a unifying thing. We are under attack. And I think we should just agree on making it clear that the Russians were trying to undermine our election and our—create discord. They were going after our election systems. We need to analyze that to figure out how do we defend better, make it more resilient, to give our citizens more confidence.

It is clear that they are trying to penetrate our energy grid and our financial sector. The next December 7 won't be planes or torpedoes coming into Pearl Harbor, it will be preceded by rolling blackouts or collapse of financial sector because of a cyberattack. And we just got to realize this. So we need to work now to make these systems more resilient.

It was clear they were trying to create discord and divide us, and I think we have fallen for it. We keep falling for the bait and beating each other up. And yet we need to know—we need to be unifying and making it clear what the Russians are doing. And it is saddening to see that we have been taking the bait and we take the bait every day attacking each other, when it is actually what—that is what the Russians want. And I think transparency and making that clear would help.

I think on the good side, I think the President has made clear in the National Security Strategy that Russia is a primary threat. And I think our defense budget that we are hoping to get done here real soon makes that clear too with our 10 percent increase in spending.

So my question at this point is, what do you think their goal is? I mean, we know that they are trying to create discord, but that is a means to an end. So what is their end? What is the purpose of the discord and the partisan divide?

General Breedlove, thank you.

General BREEDLOVE. Right back at you, sir, about your experience as a commander. Thank you.

So let me, as I think my colleague tried to do, give the press some relief. What we do now see is that institutions in America, and the press, universities and others, think tanks all around the country, are beginning to speak to what has been happening for some time. It has been a slow awakening, but people are now understanding, primarily, what Russia is doing, less so what the PRC [People's Republic of China] is doing.

But so I think we need to not be hypercritical, because folks are beginning to wake up to this. And that is the most important thing. We need to reach my brothers and sisters in small-town Georgia with this message so that they understand what is going on. And as I have said just before, I really believe that while they do have some short-term goals to try to push forward one or the other of approaches, it is really about destroying the confidence in America and American democracy, I think, in the endgame.

Mr. BACON. Do you think it is also maybe a goal to give them a freer hand with their neighboring countries? You know, what they are doing in Ukraine. If we are divided here, it is harder to come up with a unified response to other matters internationally.

General BREEDLOVE. So now I would answer sort of in the role of the former EUCOM and NATO commander. Clearly, they wanted to find cracks in our alliance, expand those cracks, live in those cracks, to destroy a unified response by the alliance.

Mr. BACON. Would you say we are in a Cold War now or is that an appropriate term?

General BREEDLOVE. I think we are in a warm war.

Mr. BACON. A warm war.

Any other comments from our two panelists?

Mr. LUMPKIN. It takes time to establish audiences. So you want to establish an audience well before you need or want to use it. You need to build the tentacles, you need to have the infrastructure; it takes time. So I think what we are seeing, in my view, is that not what is—what today is a prelude to something in the future, I just can't tell you what that is.

Mr. BACON. One of the things, it seems to counter what they are doing. We need to see what are their weaknesses. We know they are very dependent on the energy sector. They are very concerned about what we are doing in the Baltics and Poland. It just seems to me that there are some leverage points that we also have that we need to be exploring more aggressively.

But any comments with that before I——

General BREEDLOVE. In 15 seconds, I would say we need to be intellectually honest enough to know that there is two sides to every story. And we need to understand what is motivating the Russian leadership, and I am not sure that we are very good at that.

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

The CHAIRMAN. Ms. Cheney.

Ms. CHENEY. Thank you very much, Mr. Chairman. And thank you to all the witnesses. This has been very enlightening.

You know, the first thing I would say is, I think there is general bipartisan agreement you have heard, for the most part, on the committee about the threat, but I think it is really important for us to recognize that the strength of our system is debate and the

strength of our system, you know, the sort of explosion of different sources of information is not a negative. And I certainly, frankly, personally, wouldn't want to return to a time—I am not sure a time ever existed, frankly, where there was one source of information. And I do think that our adversaries have been genius in many ways at exploiting what is a strength, but people ought to have the ability to choose from different sources of information and not expect that every single source is going to be some sort of, you know, approved, verified version of the truth.

My question, though—my first question is for you, General Breedlove. You know, we are very concerned—I am very concerned that the administration has not issued—does not have any sort of a cyber policy, even though this committee has called for it. It is crucial. I am not sure how we move forward without that. But it seems to me that we have got to be in a position where we are not just thinking about what is our response to these attacks, but we are talking about deterrence, and that requires some kind of a template. And a template that says, look, there is a public diplomacy piece of this, there is an information piece of this. We need to be spreading the message about the importance of freedom and democracy. But there has got to be a line someplace where it becomes an act of war against us, an attack on the power grid, an attack on our election process.

So my question is, first of all, can you be a little bit more specific about where that line is? And, secondly, when you talk about an all-of-government approach, could you be more specific about the deterrent piece of this in terms of what are the kinds of things, even from the perspective of a declaratory policy, that we would be, you know, saying to the Russians, to the Chinese, you step over this line, these are the kinds of responses you will meet from us?

General BREEDLOVE. So thank you for the question, ma'am. I would just say that I don't label just this administration as not having these policies, these spanned administrations. We have been crying for certain policies since the first attack in Crimea, Ukraine, and other places. So these are things that I think all governments, regardless of which administration is running——

Ms. CHENEY. There is just one in the office now.

General BREEDLOVE. Right. We need these things in the tools of our soldiers, sailors, airmen, and Marines and others as they respond.

I have sort of been boring today by saying all-of-government response. We tend to, as I said, do economic things with Russia and military things in the Middle East. And I think that we need to sit down and be more direct about asking our interagency governmental process to bring diplomatic, informational, military, and economic tools in each case, and for each country there are different responses.

Ms. CHENEY. But would you be in favor, for example, General, of saying, you know, that any of our adversaries, no matter who it is, a particular kind of attack, they ought to expect that that will be met with a particular response from us that may or may not be in kind?

General BREEDLOVE. I do believe that we need to understand how to deter. I am not a huge fan of red lines, because when we

draw a red line and then we don't stand behind it, it is catastrophic. And so I would be careful in how I did that. But deterrence is in the mind of those deterred. It is less about writing something on a piece of paper. And we need to make sure we understand what gives Mr. Putin cost so that we can deter him.

Ms. CHENEY. Mr. Lumpkin, could you address this issue as well in terms of what are the kinds of things that would be most likely to deter action, and do you think that there is a particular line in terms of the kinds of actions against us that we ought to be focused on deterring?

Mr. LUMPKIN. Yeah, I think it goes back to General Breedlove's comment, you know, it depends. And it depends on if we are talking about Russia, you are talking about China, you are talking about the Iranians, each one has different points and places that pressure could be applied to have the outcomes, whether they are broad or very narrow to achieve. But what you do have to have is a process to make sure that you don't get locked into something you can't get yourself out of ultimately as you design these strategies for specific countries.

Ms. CHENEY. Thank you. I yield back, Mr. Chairman.

The CHAIRMAN. Mr. Hice.

Mr. HICE. Thank you, Mr. Chairman. And welcome and thank you for this very important hearing.

And, General Breedlove, thank you for your service and what you continue to do at Georgia Tech, and I welcome the students as well, although I am a Bulldog through and through. Glad to work with you.

I want to go back to what you were discussing a little while ago but didn't have time to get into regarding the energy. In your written testimony, you stated that Russia is using its vast energy resources to promote the dependence of its smaller neighbors and to keep them from turning to the West. Could you elaborate a little bit more on that, please?

General BREEDLOVE. So if I could just use a few examples from the Ukraine piece, and it has happened in others. When Russia is trying to bring pressure on a government, in Ukraine's case, calling in payments early, raising the price of the fuel to bring problems, or withholding delivery so that households would go cold in a very cold Ukrainian winter. So there are lots of tools they use. Russia has an elaborate, as you know, pipeline setup in eastern Europe, western Russia, in order to be very good at this, moving gas around. And so it is a tool they can use.

And then what I mentioned also in the testimony, in the Q&A, is that Russia, of course, is very keen on keeping the price of oil up because it is very much an oil-dependent economy. And so it attacks into countries like ours to prevent ventures like pipelines, fracking, other things, that would tend to suppress the price of energy. And so they are very keen to try to influence governments like ours in that respect.

Mr. HICE. Okay. So what about our potential ability to export LNG [liquefied natural gas], wood pellets, that type of thing? What kind of impact would that have?

General BREEDLOVE. Much talk about how we might in the West, larger than us, Canada and others, be a big part of reducing East-

ern European dependency on Russian energy. I believe it would be a great tool.

Mr. HICE. Okay. So a great tool on multiple fronts, obviously, for the national security of Europe. Is that what you are refer—when you say a great tool?

General BREEDLOVE. And the United States.

Mr. HICE. And the United States. All right. What other methods do we need to be aware of and have on our radar to help combat this hybrid warfare, specifically energy?

General BREEDLOVE. I will get back to you on that, sir. Right now, I think that the first and foremost on this is to be able to reduce our dependence, and now I am offering Phil Breedlove's opinion, to increase our own capacity to create. And then to offer to our allies cheap energy that we can deliver to reduce their dependence on those that would use its course of capabilities.

Mr. HICE. All right. That sounds like a great plan to me.

Do either of the others have comments on this?

Mr. LUMPKIN. No.

Mr. GARNAUT. No.

Mr. HICE. Okay. Thank you very much. I yield back, Mr. Chairman.

The CHAIRMAN. Ms. Stefanik.

Ms. STEFANIK. Thank you, Mr. Chairman. I am going to go through pretty quickly because I have seven questions and I am determined to get through all of them.

So the first one is for you, Mr. Lumpkin. Is the State Department the correct place to have this conductor? Setting aside some of the issues with the Global Engagement Center, do you believe that State is the best place for this point person to be?

Mr. LUMPKIN. I think he needs to be outside of all departments.

Ms. STEFANIK. Outside of all the departments. Okay. So what—functionally, how would that work? Would it be similar to the DNI in terms of having all the—you know, setting aside intel, having the appropriate agencies be a part of that process?

Mr. LUMPKIN. I think so. It is the only concert that I know that is cross-cutting across all departments.

Ms. STEFANIK. Okay. Within DOD, who is the conductor?

Mr. LUMPKIN. For—I mean, that is a great question, because public affairs has a conductor at DOD that it is in the information space, and you have military information operations that resides oversight at ASD SO/LIC [Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict].

Ms. STEFANIK. Right. So I ask that question to highlight something that I think we need to focus on. On the Subcommittee for Emerging Threats and Capabilities, we have quarterly briefings when it comes to CT [counterterrorism] and when it comes to cyber operations. And the briefer is able to go around the world and say globally what the threats are and what our operations are.

I fear that if we had quarterly briefings, we would not have one point person who was able to answer our questions region by region by region. So are those models that we should use as we seek to tackle IO [information operations]? So what we have worked through over the past 14 years on CT, what we are currently doing in terms of elevating Cyber Command.

Mr. LUMPKIN. Yeah. I think that the Joint Staff, J–39, which is their operation shop that is in information operations, should be able to give you and represent what each of the combatant commands is doing with regard to information operations, keeping in mind that the information operations piece supports military objectives.

Ms. STEFANIK. So do you think that is an important kind of forcing mechanism in terms of congressional oversight, thinking about having quarterly briefings on IO?

Mr. LUMPKIN. I do, and I would recommend it.

Ms. STEFANIK. Okay. What role does Cyber Command have in terms of IO?

Mr. LUMPKIN. I mean, they are—because——

Ms. STEFANIK. What role should they have?

Mr. LUMPKIN. Because they are largely in the intelligence community, not in the information space, there is a role, but it is a narrow niche.

Ms. STEFANIK. General Breedlove, you are nodding your head, I would like you to add to that.

General BREEDLOVE. It was a great question, that is what I was nodding my head to. In the end, Cyber Command is more about the medium by which information is transferred and how to adjust and control and, if necessary, defend and attack in that medium. So I was shaking my head as I was trying to think through the answer. There is not a good answer right now.

Ms. STEFANIK. All three of you referenced the strategic communications messaging strategy when it comes to countering ISIS. Can you specifically talk about how this is structured, both, you know, who the players are within DOD and State, how we work with our allies?

And then the reason I am asking that question is, if we were to identify the top threats in the IO space, I would list Russia, China, and potentially Iran, as top three. I would love to get your assessment on the specifics of how that is structured, what we can learn there, and whether you think those three threats are—where we should prioritizing having messaging strategies when it comes to those adversaries.

Mr. Garnaut, do you want to go first on that?

Mr. GARNAUT. Look, if I understood your question correctly, but let me just talk about the—so when you talk about Russia information operations, it tends to be the military piece or the cyber piece and a little bit of the astroturfing of protest movements.

China is in a broader space, and so it doesn't have a direct bureaucratic counterpart in our systems, and that is part of the problem, right? So we need to create a place where it all comes together. And I agree with Dr. Lumpkin, it has to be above the bureaucratic systems. But who—we have got to have as part of our law enforcement, you know, capability, an ability to track united front networking operations, to see it spread across all the silos of our systems, and it is much bigger than just the military piece or the cyber piece, it is a whole of public opinion emphasis.

Ms. STEFANIK. So let me rephrase my question. Since we have what you—the three of you have said is a successful strategy when it comes to countering ISIS in the information space, do we need

to come up with threat-specific equivalence when it comes to countering Russia, countering China, and countering Iran, in terms of our prioritization?

Mr. LUMPKIN. Yes. The way the construct was, is in the coalition against ISIS, we had a communications working group where we would go and we would meet quarterly, and we would sit there and hammer out, you know, the messages that audiences, and what—and how we were going to work it against a single adversary. And it was an ad hoc group, worked very, very well. But I think you have to be focused on who is the adversary and what are the outcomes you are looking for.

Ms. STEFANIK. General Breedlove.

General BREEDLOVE. So what made this coalition and this capability successful is that the leadership of our Nation and other nations in the coalition gave them the authority, responsibility, and accountability to take on the mission. And I would argue that that is what we are missing in the arrangements with Russia and China. We haven't really given one entity, like maybe the Global Engagement Center or some other entity that is uber other entities, we haven't given them that policy, authority, responsibility, and accountability.

Ms. STEFANIK. Thank you. My time has expired.

The CHAIRMAN. Thank you.

If you all will indulge me for just a couple of more probably brief questions. I am sitting here think—as I listen to all of this, I am sitting thinking about all of the effort we put into understanding the Soviet Union and the philosophy behind it and the tactics it was using around the world. It was enormous. And then it all went away. We are starting to rebuild, for example, our understanding of deterrence and thinking about these things again.

My simplified question to you all is, from kindergarten to Ph.D. level, where are we today at understanding the influence operation—I kind of like psychocultural warfare myself. Where are we in understanding what is going on to us?

General.

General BREEDLOVE. I will start with something, sir, I said to you when I was wearing a uniform. We have backed up, and probably for right reasons, not at the height of the Cold War, but when the wall fell in the early nineties, we had over 12,000 analysts on Russia. And when I testified to you in uniform the last time, we had 1,028. So we had cut our capability to look into Russia and understand Russia by 92 or so percent.

And so I would answer that we are back in junior high or maybe entering high school, and our intel communities are refocusing harvest. There are other things they are doing, sir, I think they are on it, but we have work to do.

The CHAIRMAN. Okay.

Mr. GARNAUT. Look, on China, I am not sure that we are at kindergarten yet. The amount of analytical capability we have got is so small. I can count on my hands the number of experts on Chinese influence operations, one of them is in this room, up the back, Peter Mattis, Mark Stokes, couple of people in Australia. It is thought—it is unbelievably thin, and that has got to be a major pri-

ority in building up analytical capability on Chinese politics, Chinese history, and patterns of hybrid warfare.

The CHAIRMAN. Just briefly, based on your experience, is there the appropriate exchange between analytic experts here and in our most valued allies, like Australia, on this issue?

Mr. GARNAUT. Well, yes. I think the flow of information analysis is really quite strong between Australia and the United States. This is a topic that comes up often. But we just don't have the depth of capability. We don't have enough to share at this stage.

The CHAIRMAN. Okay. Mr. Lumpkin, what grade are we in?

Mr. LUMPKIN. I was going to address the Iran issue, and I would say we are probably in middle school somewhere.

The CHAIRMAN. In where?

Mr. LUMPKIN. In middle school, junior high as well, just because of the number of resources we have against it. It is very small.

The CHAIRMAN. I just want to go back at the end to the central purpose of this committee, and that is overseeing the Department of Defense and the U.S. military. Taking all of your points about whole-of-government, the importance of intelligence in law enforcement and all of that, can you provide just a few comments on the role of the United States military in dealing with the problems that we have discussed today?

General BREEDLOVE. I don't want to pump sunshine, but I would offer to you that there are some really brilliant people working hard on this issue. And I have absolute trust and confidence in Joe Dunford and in our Secretary of Defense, because I have watched them, served with them, et cetera, over the years. And I know that inside of the Joint Staff, General Dunford is doing some work on trying to reorganize around Russian issues. I led one of those efforts in uniform. And Harry Harris, as the commander of PACOM [U.S. Pacific Command], led a similar issue as we looked at China. And building a broader rubric under which to address these than just the combatant commanders, and reaching out in those processes to other governmental agencies to bring them in.

So, sir, I am encouraged by what I see inside of our DOD and our uniform military services on how they are approaching this.

Mr. LUMPKIN. And, sir, the Department of Defense is carrying a lot of water on this front. They are carrying a lot of water for the interagency. But everything can't be tied back to a military objective, and that is where we fall short. Our gaps and seams are massive. And the GEC, frankly, and during my tenure, would not have been functional at all if it wasn't for the detailees that came over from the Department of Defense because the positions themselves weren't resourced within the building.

So, again, I think the U.S. Government's efforts are maturing, but the Department of Defense is doing a lot of the heavy lifting for us.

The CHAIRMAN. Mr. Garnaut, in a broader sense, military role in this space?

Mr. GARNAUT. Look, I think military systems and defense departments have had to pull too much weight here, because—almost by default because the rest of the system haven't been carrying their weight.

The CHAIRMAN. Yeah. I think that's definitely true here.

Mr. GARNAUT. Especially the law enforcement piece.

The CHAIRMAN. Okay. All right. This has been very helpful. Thank you all for being here. A lot of insight is gained. We really appreciate you all taking the time to be with us today.

The hearing stands adjourned.

[Whereupon, at 12:40 p.m., the committee was adjourned.]

A P P E N D I X

MARCH 21, 2018

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 21, 2018

Statement of Chairman William "Mac" Thornberry
House Armed Services Committee Hearing:

State and Non-State Actor Influence Operations: Recommendations for U.S. National Security

March 21, 2018

Whether the term used is "political warfare," "influence operations," "psycho-cultural warfare," "indirect warfare," "hybrid warfare," or one of many others that has been suggested, it is clear that the United States and our allies are under consistent attack using non-kinetic tactics intended to undermine and weaken us.

We know that Russia intervened in a variety of ways to sow dissension during the 2016 election. History and now declassified documents establish that the former Soviet Union had a track record of "active measures" against NATO's deployment of intermediate range missiles in Europe, and they included providing propaganda themes to peace movement groups, as well as organizational expertise, financial resources, forged U.S. military documents, etc. And according to declassified CIA documents, that campaign was built upon a similar campaign they carried out against the proposed neutron bomb of 1977-78.

It's part of the standard playbook, and we should expect more of the same against the decisions called for in the Nuclear Posture Review, for example, only given their recent success, a more sophisticated version.

While most of the attention has been centered on Russia as the source of these attacks, they are not the only adversary using such methods. China has spent billions of dollars to gain economic leverage, buy access to infrastructure, and shape public opinion and perceptions around the world to its advantage. Iran, various terrorist organizations, and even North Korea make use of some of them.

These tactics challenge our traditional ways of thinking about warfare; they challenge our organizational structure on who is responsible for defending the country in this sphere; and they challenge our ability to develop and use the tools needed to counter them in a timely way.

As the National Defense Strategy says, "China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other nations' economic, diplomatic, and security decisions." It is important to identify the motive behind these efforts, but the question remains whether we have the tools, organizations, and approaches to protect American sovereignty and national security.

We hope to gain insight into these issues from our distinguished panel of witnesses.

Statement of Ranking Member Adam Smith
House Armed Services Committee Hearing:

State and Non-State Actor Influence Operations:
Recommendations for U.S. National Security

March 21, 2018

Thank you, Mr. Chairman for hosting today's hearing and welcome to the witnesses. I look forward to hearing your views on influence operations, the impact of such operations to U.S. national security, and recommendations for countering and deterring campaigns that undermine U.S. and allied interests.

Violent extremist organizations have used propaganda to recruit, inspire, and spread their message for decades. Terrorists have filmed videos and recorded messages in ungoverned spaces in the Middle East and Southwest Asia, intended to shape the narrative for tactical, operational, and strategic gain.

In recent years, ISIS has demonstrated a greater degree of sophistication in spreading its message and in manipulating information to achieve desired objectives on and off the battlefield. This was evidenced by the large number of volunteers recruited from across the globe and ISIS' ability to inspire terrorist attacks outside of its territorial strongholds, as well as through ISIS use of publicly available information to target key military members, agency officials, and others.

State-actors also have a history of using influence activities as a means to an end. The Nazis had a Ministry of Propaganda. During the Cold War, the Soviet Union and other communist countries used influence, through proxies and propaganda, to spread their ideology.

However, the global information environment of today provides an opportunity for countries like Russia and China to exploit information and to spread disinformation to mass audiences on a scale that was previously unimaginable. You don't have to look far for an example—Russia is conducting a campaign to undermine American democracy and other democratic institutions in Europe. As I stated last week, Russia's destabilizing actions are becoming ever more apparent.

Influence activities are not just taking place in the information environment. Russia is backing political candidates, employing proxies, conducting cyberattacks, and using unconventional methods to achieve its goals and objectives. China leverages economic suasion to further foreign policy objectives that don't necessarily adhere to the international rules-based order.

Country-specific responses aren't enough to address these challenges. Confronting and deterring holistic influence campaigns spanning military, economic, political, and social bounds requires a holistic response. We must leverage all instruments of national power across the whole-of-government, including the Department of Treasury, Department of Education, elements of the Intelligence Community, and the Department of State.

Yet, there appears to be no concerted effort at the highest level of government to come up with a sound strategy that counters and deters influence campaigns, advances U.S. interests, achieves strategic effects, and remains in line with our ethics and core values. This is not only disappointing, but extraordinarily dangerous.

I look forward to working with my colleagues on this committee and others, to continue to move the ball forward on this issue.

Thank you, Mr. Chairman.

Atlantic Council

Russian Interference in Domestic Politics

Prepared statement by

General Philip M. Breedlove USAF (Ret)

Distinguished Professor, Sam Nunn School, Georgia Institute of Technology
Board Director, The Atlantic Council of the United States
Former NATO Supreme Allied Commander Europe; Commander, US European Command

Before the

United States House Committee on Armed Services
United States House of Representatives
115th Congress

Good morning, and thank you Chairman Thornberry, Ranking Member Smith, and members of the Committee for the opportunity to speak with you about Russian interference in democratic politics. The Russian interference in the 2016 US Presidential Election is deeply troubling, yet unsurprising. It is up to us as Americans to acknowledge the threats that Russian disinformation provides, and develop the effective strategies needed to combat them.

This weaponization of information by Russia is not new; in fact, it dates back to the Soviet Union. In 1983, a pro-Soviet newspaper in India published an article accusing the Department of Defense of creating AIDS in an attempt to develop new biological weapons. In 1964, the KGB used similar tactics in an effort to convince the Indonesian President that there was a CIA plot to assassinate him. The primary differences between these disinformation campaigns and those today, is twofold: firstly, the internet and social media make it much easier to spread disinformation, and secondly, these campaigns are increasingly targeting first world Western nations.

Russia took full advantage of this new media landscape by promoting disinformation to sow discontent among Americans. Russia exploited divides in the American populace to promote what many have referred to as a "culture war". Surveys have shown that the US is more polarized than it has ever been on issues such as gun control, immigration, religion, and race. Russian operatives, seeing an opportunity, purchased social media advertisements and created social media profiles, in order to promote partisan stances on these issues to further widen the rift. Russian advertisements and profiles did not have a consistent political position; the only consistent aspect is that they all promoted partisan positions on immensely divisive issues.

The details of Russia's interference in the election are maddening. However, the reality is that we should not be surprised by this interference. The Russians have interfered with numerous elections in Western nations recently, including those in the Netherlands, Germany, and France. There is increasing evidence that Russia worked to influence the referendum in which the United Kingdom decided to leave the European Union, as recently shown in a report prepared by some on the Senate Foreign Relations Committee. It has promoted anti-immigration sentiment in Europe, by creating and spreading the story of "poor Lisa," a thirteen-year-old girl who, as the fallacious story goes, was abducted and raped by migrants.

Furthermore, we have "meddled" in elections in our own way. In 1953, Allen Dulles offered $5 million to an agent to sway the Filipino elections. 1958's Operation Booster Shot encouraged rural Laotian farmers to vote against Communist politicians in Laos. This meddling did not end with the Cold War; in the 2006 Palestinian elections in Gaza, the United States provided economic assistance in an attempt to bolster Fatah's chances. The reality is that both the United States and Russia have meddled, and we should not be surprised by this trend continuing.

What is astounding about Russian meddling is how brazen Russia was in executing it, as well as the fact that Russia seems to believe that it can escape this with its reputation unsullied. Russia appears to be surprised by the outrage that has been seen throughout the US. The US has been a leader and pillar of Western democracy, and the fact that Russia believed that it could interfere with American elections with no response is truly shocking.

However, Russia's interference in the 2016 US Presidential Election is merely a symptom of a larger hybrid war against the West, in which economic, cyber, and disinformation tactics are used in conjunction with conventional forces in order to exert force or pressure on an adversary. In February 2013, General Valery Gerasimov, Chief of the General Staff of the Armed Forces of Russia, gave a speech entailing this strategy, claiming:

> The very 'rules of war' have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures—applied in coordination with the protest potential of the population.

This led to the coining of the term "the Gerasimov Doctrine." This describes Russia's view that warfare is not simply a conventional affair, but one that uses the aforementioned cyber, economic, and information tactics.

This is notable because it shows that Russia acknowledges that its election meddling is a form of warfare. While Russia may deny that it interferes with elections, or claim that it is innocuous, the words of General Gerasimov ring loud and clear: disinformation efforts are efforts of warfare.

The reality is that Russia is using hybrid tactics to target Western values, democratic governments, and transatlantic institutions. President Vladimir Putin claimed in a state of the nation address that the collapse of the Soviet Union was a major geopolitical disaster of the twentieth century. Russia sees the West, and in particular, a unified West, as an adversary. Waging a conventional war against the West would be unfavorable to Russia. As such, it has used hybrid warfare to break up Western unity.

Exploiting divisions in US society and promoting a "culture war" is one key element of Moscow's efforts to weaken the West. Through disinformation, it has plied differences in Europe to promote Euroscepticism and to grow the notion among the peoples of Europe that the EU is not beneficial to them. It has waged cyber-attacks, such as the NotPetya attack in Ukraine in 2017, the Fancy Bear attack on German Members of Parliament earlier this month, or the numerous distributed denial of service (DDOS) attacks on the Estonian government. It has used economic subversion to exploit the relatively smaller economies of its neighbors to subvert political power.

It uses its vast energy resources to promote the dependence of its smaller neighbors, working to keep them in the Russian sphere of influence and preventing them from turning to the West. In short, while the 2016 Presidential Election is the most notable case of Russian hybrid warfare, especially for Americans, it is not the only case of Russian hybrid warfare.

The Russian interference in the 2016 US Presidential Election has received an unprecedented amount of media coverage. However, we should not be so myopic as to see this interference in a vacuum. In order to effectively combat said interference, we need to understand the scope of Russian hybrid warfare. We need to view this as a comprehensive problem that connects the dots of recent Kremlin activity. We cannot simply

take a stance against a specific case of election interference, we must take a stance against Russian hybrid warfare in its entirety. In all the cases of Russian disinformation and election interference, the West has been slow to see it, and even slower to react. We need to move past simply trying to formulate a reaction to interference in the Presidential Election, we need to move to a place where we are ready to combat hybrid warfare and not need to react at all.

Hybrid warfare is a form of warfare that the United States has yet to fully understand, never mind prepare for. The revelation of Russian disinformation in the election is the wake-up call that hybrid warfare is occurring, even if we are unwitting participants in it. Simply condemning the election meddling is not going to solve this problem, and it is not going to prevent future Russian hybrid operations. We must treat this with the gravity that it deserves. We need to take a position, establish policy, and execute it. The Russian hybrid threat is larger than the 2016 Election, and larger than the United States. It is a threat to liberal order that the West has become accustomed to, and it will continue to be until we develop an effective strategy and implement the necessary policies to combat it. Thank you, and I look forward to your questions.

Philip Breedlove

Gen. Philip M. Breedlove, USAF, Ret., is a proven strategic planner, motivational leader and talented communicator. He is a highly decorated retired general of the U.S. Air Force where he reached the highest levels of military leadership as one of six geographic combatant commanders and the Supreme Allied Commander of NATO.

During 39 years of service, General Breedlove served in a variety of demanding command and staff positions, leading large-scale, diverse, global operations across two theaters of combat and earning a reputation as an inspirational leader focused on his people, their families and mission accomplishment. Leading a diverse political- military alliance, he was able to build consensus and form teams to accomplish complex tasks spanning multiple continents.

As the Supreme Allied Commander Europe and the Commander of U.S. European Command, he answered directly to NATO's governing body, the North Atlantic Council, and to the President of the United States and Secretary of Defense. He led the most comprehensive and strategic structural and policy security changes in the alliance's 70-year history. His diplomatic skills reassured allies, deterred potential aggressors and maintained alliance unity during the most dynamic and challenging period since its inception. He led the forces of 28 nations and multiple partners in ensuring the security of an alliance that accounts for more than half the world's gross domestic product.

As Commander, U.S. Air Forces Europe and Air Forces Africa, General Breedlove was responsible for organizing, training, equipping and maintaining combat-ready forces while ensuring theater air defense forces were ready to meet the challenges of peacetime air sovereignty and wartime defense. This diverse portfolio included both theater and operational air and ballistic missile defense, areas where his operational designs remain in place today.

As Vice Chief of Staff of the Air Force, he presided over the Air Staff and served as a member of the Joint Chiefs of Staff Requirements Oversight Council and Deputy Advisory Working Group during a period of intense challenge, including devising measures to meet the requirements of the Budget Control Act's required $480 billion reduction of the Department of Defense budget. Accordingly, he led the organization, training and equipping of more than 690,000 people serving in the U.S. Air Force and provided oversight of its $120 billion annual budget.

As Assistant Chief of Staff for Air Operations, Plans and Requirements, General Breedlove directed all Air Force operations across the globe, oversaw strategic and operational planning, and set the requirements for all Air Force procurement. Additionally, he was one of two original authors of the Defense Department's Air-Sea Battle Concept.

General Breedlove served in a variety of assignments leading up to those leadership positions, including commanding a squadron, a group, three fighter wings and a numbered Air Force in service across three different continents. His extensive command and control experience in wartime, contingency planning, and humanitarian relief actions include operations in Africa, Asia and the Middle East.

He earned his Bachelor of Civil Engineering degree from the Georgia Institute of Technology and a Master of Science in aerospace technology from Arizona State University. Additionally, he completed a Masters of International Security Affairs from the National War College, a Fellowship in International Security Affairs, Seminar XXI from the Massachusetts Institute of Technology and completed Leadership at the Peak at the Center for Creative Leadership, Colorado Springs.

General Breedlove currently serves on the Georgia Tech Advisory Board, as a Distinguished Professor in the Sam Nunn School of International Affairs at Georgia Tech, as a Senior Advisor

to Culpeper National Security Solutions and on the Board of Directors of the Atlantic Council.

Retired from the Air Force in 2016, General Philip M. Breedlove's active duty biography is available on the Air Force website.

Testimony to US House Armed Services Committee, 21 March 2008.
John Garnaut, in personal capacity.

Chairman Thornberry, Ranking Member Smith, and distinguished Members of the Committee. It's an honour to be here. Thank you for the generous invitation to talk with you all today.

To understand the mechanics of China's international influence we need to look beyond the gravitational pull of the Chinese economy and the war-fighting power of the People's Liberation Army. Both are important. But neither are as important as the world of influence and interference which sits between those two poles. This is the domain in which the Chinese Communist Party manipulates incentives inside our countries in order to shape the conversation, manage perceptions and tilt the political and strategic landscape to its advantage.

The party works hard to find common interests and cultivate relationships of dependency with chosen partners. The modus operandi is to offer privileged access, build personal rapport and reward those who deliver. From open source materials we know this is happening in universities, in business communities, in ethnic Chinese communities, in media and entertainment, and in politics and government. But the Communist Party institutions, ideologies and methodologies involved are so alien to our systems that we have been having trouble seeing them let alone responding. The party has been "winning without fighting", to borrow some of its terminology.

However, under the uncompromising leadership of President Xi Jinping, China's activities have become too brazen and aggressive to continue to ignore. A re-evaluation is taking place in half a dozen established democracies around the world, including Australia and the United States. Many more are entering the conversation.

I have described the Australian experience in a Foreign Affairs article which is attached to my written submission and I won't it duplicate now. But there is one point I'd like to underscore - and that is the vital importance of maintaining principles, analytical clarity and strategy.

Our challenge - the shared challenge of democracies across the world - is to work with the strengths and shore up the vulnerabilities of our open, multicultural, democratic systems in order to push back against authoritarian interference. We need a rigorous and principles

approach that is capable of securing a broad and durable consensus within countries and between them.

We need to identify and conceptually separate the "black" from the "white" while recognising that there is a large grey area of ambiguity and plausible deniability that sits in between. This requires a great deal of empirical work, both in and outside government.

Once we have an empirical baseline, and clarity about which categories of activity we care about and how much we care, then we can design a surgical response that manages the risks and targets the harm without hurting ourselves.

In my view, we should continue to welcome ordinary diplomacy, transparent public diplomacy and economic activity that does not come with strings attached. I doubt we could lift the drawbridge and cut ourselves off from the world even if we wanted to.

But wherever covert, coercive, or corrupting elements are involved - when legitimate and transparent forms of influence cross the line into harmful "interference" - then we need to respond.

Shutting down the black is primarily a counterintelligence and law enforcement challenge. An enormous one, I might add.

But this won't be enough on its own.

We also have to build transparency and accountability mechanisms to illuminate the vast array of grey. We need to reinforce and re-ativate the antibodies of our civil societies - the natural antibodies which the party has been working to disable and suppress.

In Australia, the Turnbull Government is developing a counter-interference strategy that is built upon the principles of sunlight, enforcement, deterrence and capability. The strategy is country-agnostic in that it is designed to apply to any country's misbehaviour, not just China's.

The strategy includes new legislation to tackle the black and also the grey. One set of laws introduces tough but graduated criminal provisions against political interference and espionage. Another set of laws imposes disclosure obligations for those working in Australian politics on behalf of a foreign principal – this is an upgraded transparency regime

loosely modelled on your Foreign Agents Registration Act. Importantly, enforcement activities are also being brought into a central integrated hub.

But this is only the very early stages of a difficult struggle to reinforce the integrity of our democratic processes. There is an enormous body of hard work to be done. I'm very much looking forward to the discussion.

March 9, 2018

How China Interferes in Australia

And How Democracies Can Push Back

John Garnaut

JASON LEE / REUTERS

The Australian flag flutters in front of the Great Hall of the People during a welcoming ceremony for Australian Prime Minister Malcolm Turnbull in Beijing, China, April 2016.

Australia is the canary in the coal mine of Chinese Communist Party interference. Over the past 18 months, the country has been shaken by allegations of the Chinese party-state working to covertly manipulate the Australian political system and curate the wider political landscape. There are claims of Beijing-linked political donors buying access and influence, universities being co-opted as "propaganda vehicles," and

Australian-funded scientific research being diverted to aid the modernization of the People's Liberation Army (PLA). Most notoriously, an ambitious young senator, Sam Dastyari, was exposed for parroting Communist Party talking points and giving countersurveillance advice to a Chinese political donor before being hounded into premature retirement.

The scandals might seem odd. Few countries on the planet have benefited as clearly from China as Australia has. Its society has been enriched by waves of Chinese migrants and sojourners for 160 years. Its national income grew as much as 13 percent in a single decade as a result of China's resource-intensive construction boom, according to the Australian Reserve Bank. And an easing of the resources boom has been offset by the spending power of 180,000 Chinese students and a million tourists each year, along with hundreds of thousands of migrants who have mostly thrived in their new country.

Yet these are the very ingredients that make Australia's debate over Chinese influence so interesting. Nobody knows what happens when a mid-sized, open, multicultural nation stands its ground against a rising authoritarian superpower that accounts for one in every three of its export dollars. Even the firebrand editorial writers of China's tabloid press seem unsure. "Australia calls itself a civilized country, but its behavior is confusing," The Global Times wrote. "While it is economically dependent on China, it shows little gratitude."

The Australian conversation has evolved from amorphous anxieties about Chinese influence and soft power into more precise concerns about covert interference by the Chinese Communist Party. Media reports are shedding light upon a hidden world of inducements, threats, and plausible deniability. They reveal a dimension of risk that sits between the poles of economic attraction and military force, which Western Sinologists, diplomats, and national security officials had not previously focused on. The more we learn, the more it

seems that there is little that is soft about the way the party wields power beyond its borders.

The distinctive part of the Australian experience is not what China is doing there but how Canberra is pushing back in the face of threats from Beijing.

The distinctive part of the Australian experience is not what China is doing there but how Canberra is pushing back in the face of threats from Beijing and pressure from local business leaders worried about economic retaliation. Clarity of diagnosis has set the stage for a surgical response—one that manages the risks and targets the harm while attempting to maintain the overall project of engagement. This is not an easy balance to strike, but Australia's efforts to do so should be closely watched by leaders from Washington, Auckland, Ottawa, and Berlin—who may soon find themselves in a similar position.

CHINESE AUSTRALIANS LEAD THE DEBATE

Key to the party's operations in Australia is collapsing the categories of Chinese Communist Party, China, and the Chinese people into a single organic whole—until the point where the party can be dropped from polite conversation altogether. The conflation means that critics of the party's activities can be readily caricatured and attacked as anti-China, anti-Chinese, and Sinophobic—labels that polarize and kill productive conversation. And it is only a short logical step to claim all ethnic Chinese people as "sons and daughters of the motherland," regardless of citizenship.

Yet contrary to claims of Sinophobia, the Australian debate has from the beginning been anchored in the community of Chinese Australians. Ethnic Chinese writers, entrepreneurs, and activists have led in drawing the nation's attention to the

party's efforts to suppress the diversity of their opinions through surveillance, coercion, and co-option.

In 2005, Chinese defector Chen Yonglin exposed an enormous informant network that kept tabs on Chinese Australians, including Falun Gong practitioners, who defied the party line. He explained how he would use the information to take targeted coercive actions like confiscating passports, denying visas, and shutting down meetings. In 2008, Chinese Australian writer Yang Hengjun illuminated the party's efforts to mobilize thousands of red-flag-waving students to march on Canberra's Parliament to "defend the sacred Olympic torch" against pro-Tibet and other protestors, as the torch wound its way to the Olympic ceremony in Beijing. After the 2009 arrest of Australian iron ore executive Stern Hu, several Chinese Australian entrepreneurs revealed that they were targeted by the Chinese security system in ways that other Australians were not. They were all jailed on trumped-up charges, stripped of their assets, and mistreated during interrogations. The Kafkaesque tragedy of Matthew Ng, Charlotte Chou, and Du Zuying became front page news in Australia because they and their families chose to tell their stories.

More recently, Chinese Australian journalists have laid a foundation of investigative reporting on the party's concealed links to Australian politics. Philip Wen, Beijing correspondent for The Sydney Morning Herald, showed how the party was "astroturfing" grassroots political movements to give the impression of ethnic Chinese support for Beijing's policies and leaders and to drown out its opponents. He also discovered that Australian politicians did not know basic details about Chinese citizen political donors who were bankrolling their campaigns, including their real names. Student journalist Alex Joske, who owes his Chinese language fluency to his Beijing-raised mother, has mapped the party's "united front" networks and shown that they are now so ubiquitous—and well-resourced—that they are crowding out

independent opportunities for ethnic Chinese community and political representation. He's also shown how those networks can be activated to silence Chinese Australians, including his own experience of being intimidated by leaders of the local Chinese Students and Scholars Association.

And for every story of state-sponsored coercion and co-option that Chinese Australians publicize, there are dozens that never surface. One journalist told me how he'd been summoned to a karaoke bar and physically assaulted in retaliation for his report on the dealings of a Chinese state-owned company in Australia. Another gave a parliamentary committee a confidential dossier detailing how Beijing sought to choke one of Australia's last independent Chinese-language media platforms by intimidating its advertisers. In this case, one China-based advertiser was forced to stop after a Ministry of State Security official camped in its office for two weeks. Another, in Australia, agreed to stop after being invited to a three-hour "tea" session at a Chinese consulate in Australia. At the same time, pro-Beijing media proprietors are rewarded with free content, equipment, and business opportunities.

VULNERABILITIES TO INTERFERENCE

The Chinese Communist Party invests enormous resources in shutting down discordant voices and providing incentives to develop more favorable ones. The party's United Front Work Department, which, according to former U.S. intelligence analyst Peter Mattis, seeks to "mobilize the party's friends to strike at the party's enemies," reaches not just into Australia's Chinese diaspora but also beyond, through front organizations such as the Australian Council for the Peaceful Promotion of Reunification of China. Similarly, the PLA intelligence system operates platforms, such as the China Association for International Friendly Contacts, that work to outsource the party's messaging by finding common ground

with self-interested or naive intermediaries. The modus operandi is to offer privileged access, build a personal rapport, and reward those who faithfully recite the suggested talking points.

Authoritarian interference probes and exploits different vulnerabilities of democracies in different ways. Australia's vulnerabilities include broken funding models for universities and media, uniquely lax campaign finance laws, and a special egalitarian disrespect for retired politicians. Interference activities corrode the trust that makes open, democratic, and multicultural systems work. They can corrupt political processes. And to the extent that they impact directly on the parliamentary system, they cut to the core of sovereignty itself. In May of last year, Meng Jianzhu, then China's security chief, warned the Labor opposition leadership about the electoral consequences of failing to endorse a bilateral extradition treaty. According to The Australian newspaper: "Mr Meng said it would be a shame if Chinese government representatives had to tell the Chinese community in Australia that Labor did not support the relationship between Australia and China."

In some Australian quarters, the party's predilection for shutting down critical voices has become deeply internalized. The first book-length treatment of Chinese influence work—Clive Hamilton's Silent Invasion—was shelved by three successive publishers over preemptive fears of retaliation by Beijing. Similarly, Australian university leaders have publicly dismissed concerns about improper Chinese pressure—including from their own scholars—while simultaneously launching a fence-mending mission to soften the economic retaliation that they fear is coming.

CANBERRA STEPS UP

In recent months, the conspiracy of silence has been

punctured by a catalytic process in which journalists, scholars, security officials, and politicians have all started to learn from each other. The process has involved security agencies communicating warnings to the public more clearly than before; journalists building on those warnings and drawing upon scholarly expertise; and politicians taking security agencies and credible media investigations seriously.

In June 2017, a joint investigation by the Australian Broadcasting Corporation and Fairfax Media revealed that the Australian Security Intelligence Organization (ASIO) had warned the major political parties that two of Australia's most generous donors had "strong connections to the Chinese Communist Party" and that their "donations might come with strings attached." One of them leveraged a $400,000 donation in an attempt to soften the Labor Party line on the South China Sea. A Fairfax reporter, Nick McKenzie, also revealed that a Liberal trade minister had stepped directly from office into a consultancy job at a party-linked company, earning $880,000 a year for unspecified services.

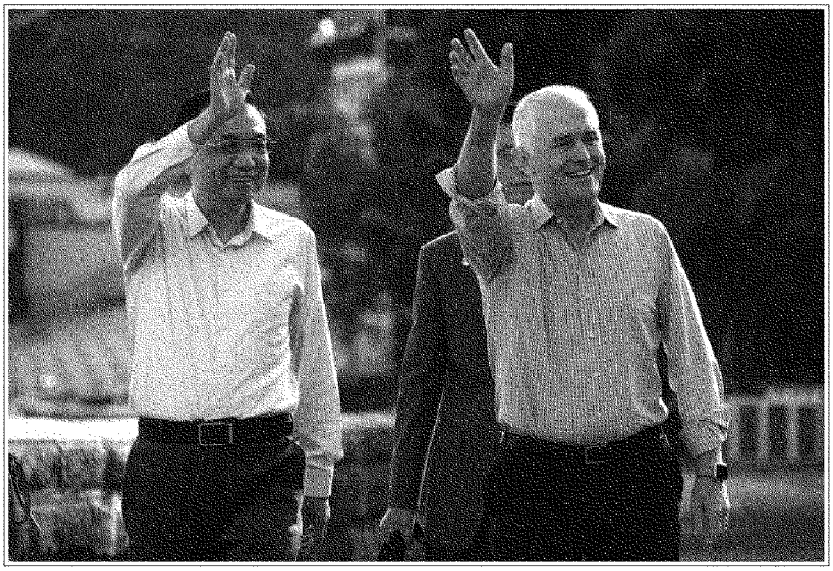
Late last year, as the media reports kept rolling in, Prime Minister Malcolm Turnbull's Liberal coalition government declared political war on Senator Dastyari's collaboration with an "agent of a foreign country." By then, Dastyari had been shown to have recited Beijing's South China Sea talking points almost word for word, immediately after his benefactor had threatened to withdraw a $400,000 donation. He had counseled the Chinese citizen donor—whom ASIO had labeled as a security risk—to place his phone aside to avoid surveillance of their conversation. The Turnbull government's attacks served a partisan political purpose, but they also brought the question of foreign interference into the mainstream conversation and, for the first time, showed that there were limits to acceptable conduct.

Turnbull also revealed that he'd commissioned a classified

investigation into foreign interference in August 2016. The findings had "galvanized" the government to map out a strategy shaped by four principles. First, a counter-foreign-interference strategy would target the activities of foreign states and not the loyalties of foreign-born Australians. As Turnbull put it, "Our diaspora communities are part of the solution, not the problem." Second, the strategy would be country agnostic and not single out Chinese interference. Third, it would distinguish conduct that is "covert, corrupting, or coercive" from legitimate and transparent public diplomacy. And fourth, it would be built upon the pillars of "sunlight, enforcement, deterrence, and capability." Turnbull introduced legislation that banned foreign political donations; imposed disclosure obligations for those working in Australian politics on behalf of a foreign principal; and introduced tough but graduated laws against political interference and espionage. (Days after Turnbull introduced these new laws, reports suggested that Beijing may have activated its United Front networks to campaign against the "ant-China, anti-Chinese" ruling Liberal coalition in a crucial by-election.)

According to one opinion poll, two-thirds of voters support the foreign interference legislation, with just 11 percent opposed. Elite opinion, however, seems skewed the other way. University, media, and business organizations have accused the government of overreach and argued for exemptions. The government has conceded ground—carving "media" out of some secrecy and espionage offences—and it may go further after a parliamentary committee delivers its review at the end of this month. Some critics say that the government has failed to explain the interference problem, others that it has been too negative about Australia's relationship with China. Many are concerned that loose language and allegations can too easily taint all ethnic Chinese people. Some are even more harsh and dismissive. Sydney University Vice Chancellor

Michael Spence, for example, has said that the Turnbull government should stop its "Sinophobic blatherings."



DAVID GRAY / REUTERS

Australian Prime Minister Malcolm Turnbull waves with Chinese Premier Li Keqiang to members of the public as they walk along the Sydney Harbour foreshore in Australia, March 2017.

THE DEMOCRATIC WORLD'S PATH FORWARD

The Australian polity has become alive to a threat that other nations share but are only starting to recognize and confront. This recognition has been assisted by the sheer brazenness of Chinese President Xi Jinping's drive for global influence and by watching Russian President Vladimir Putin and his agents create havoc across the United States and Europe. In the aftermath of the U.S. presidential election, it is far more difficult to dismiss foreign interference as a paranoid abstraction.

The Australian polity has become alive to a threat that other nations share but are only starting to recognize and confront.

If Australia has "woken up" the world on China's interference, as a senior Pentagon official puts it, it has been able to do so for five reasons. First, the debate originated inside the Chinese Australian community and has distinguished what the party is doing from its subjective impact on those it targets. Second, Australia has sidestepped important but unproductive normative arguments about what China "is" and instead focused on empirical questions about what the Chinese party-state is doing. Third, the government commissioned a thorough cross-agency investigation that supported a firm internal consensus. Fourth, participants have worked hard to define the line that separates legitimate influence in an open society from intrusive interference. Finally, the principles are framed to apply equally to all countries that engage in covert, corrupting, or coercive behavior.

Turnbull aims to build a consensus around the defense of core democratic values and institutions, something Australia's opposition Labor Party is likely to support. And Canberra is increasingly finding common cause with other democracies, including the United States. But there is a very long way to go.

Australia and the democratic world need to reinforce independent Chinese-language media platforms so that diaspora communities are not forced to rely on news that has been filtered by Beijing. Universities need new processes to ensure transparency, restore the integrity of research, and rebuild China literacy. Journalists, writers, and politicians need to avoid loose generalizations that make it easier for the party to make its case against them. And diplomats need to ensure that the relationship with China is a tool for achieving

national objectives, not an end in itself.

Intelligence agencies have begun to articulate their concerns, but they now need to go further. Warning about an abstract risk to "sovereignty" is not as helpful as explaining the modus operandi. And although U.S. agencies may be following Australia's lead, Australian agencies should borrow from the playbook of Special Prosecutor Robert Mueller and use the prosecution process as an opportunity to advance public education. To date, journalists and politicians have had to carry too much of the load.

Australia has no choice but to work with the strengths and shore up the vulnerabilities of its open, multicultural, democratic system. It will match spies against spies when it has to. But, like all liberal democracies, it will only truly succeed when it can battle it out with evidence and reasoned argument on open terrain.

JOHN GARNAUT is the founder of JG Global, a strategic risk advisory. He previously worked as China correspondent for Fairfax Media and was Senior Adviser to Prime Minister Malcolm Turnbull.

STATEMENT OF

HONORABLE MICHAEL D. LUMPKIN

VICE PRESIDENT

LEIDOS HEALTH

BEFORE 115TH CONGRESS

HOUSE ARMED SERVICES COMMITTEE

Introduction

Chairman Thornberry, Ranking Member Smith, and distinguished members of the Committee, thank you for this opportunity to address you today as a private citizen and in a personal capacity on the topic of "State and Non-State Actor Influence Operations: Recommendation for U.S. National Security". My knowledge on this topic stems from my time as an employee of the U.S. government and I currently do not work in the field of information operations nor have I received, directly or indirectly, any compensation for work in the field since departing government service in January 2017. That said, I trust my experience as a career special operations officer, Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, and Special Envoy and Coordinator for the Global Engagement Center (GEC) at the Department of State will be helpful in providing perspective as Congress assesses the U.S. government's strategy, capabilities and overall effort towards countering state and non-state sponsored propaganda and influence operations.

From my time leading the GEC, I'm familiar with the bicameral interest and bipartisan engagement by Members of Congress on these important issues. First established by Executive Order 13721, the mission of the GEC was expanded by the 2017 National Defense Authorization Act (NDAA) to include counter-state propaganda and disinformation efforts, well beyond its original charter which directed the Center to diminish the influence of terrorist organizations such as the Islamic State of Iraq and Syria (ISIS) in the information domain. This congressional mandate was a big step in the right direction; for the first time a single entity was charged with leading, synchronizing, and coordinating efforts of the Federal Government towards countering foreign state and non-state disinformation efforts.

I believe Congress has correctly identified such information operations as an ongoing and persistent threat to U.S. national security interests. Unfortunately, and based on my previous experience in government, I am similarly convinced that we are still far from where we ultimately need to be in order to successfully protect and defend those national interests in the modern information environment.

I am very pleased to be joined here today by General Phil Breedlove and Mr. John Garnaut. I believe we are collectively postured to address your questions on the issue at hand.

The Current Situation

Since the end of the Cold War with the Soviet Union, which arguably was the last period in history when the U.S. successfully engaged in sustained information warfare and counter-state propaganda efforts, advances in technology have enabled instantaneous global communications; we are living in a hyper-connected world where the flow of information moves across borders in real time and across traditional and social media platforms. The lines

of authority and effort between public diplomacy, public affairs, and information warfare have blurred to the point where in many cases information is consumed by U.S. and foreign audiences at the same time via the same methods.

While the means and methods of communication have transformed dramatically, most of the laws and policies governing how the U.S. government responds to sophisticated information operations and disinformation campaigns by foreign adversaries have remained unchanged. It is true that there has been some tinkering and tweaking, but nothing substantive or transformational. Put simply, our institutions have not kept pace with the evolving threats.

Lack of Accountability and Oversight

Antiquated bureaucratic structures and traditional lines of authority remain a significant impediment to progress. To date, there is not a single individual in the U.S. government below the President of the United States who is responsible for managing U.S. information dissemination and providing strategic guidance for how to confront our adversaries in the information environment. While the 2017 NDAA mandated that GEC lead, organize, and synchronize U.S. government counter-propaganda and disinformation efforts against state and non-state actors abroad, it failed to elevate the head of the GEC to a position of authority commensurate with its expansive mission. The GEC operates at the Assistant Secretary level and lacks the necessary authority to direct the Interagency. In practice, this means that the GEC is considered at best a peer to a half dozen regional or functional bureaus at the State Department and numerous disparate organizations at the Defense Department, to say nothing of the other departments and agencies that have an important stake in this fight. Simply put, although the GEC is directed by law with the mission to lead the Interagency, the practical reality is that its role is reduced to simply a "suggesting" function which agencies can choose to follow or not follow as they see fit. The result is a significant misalignment of responsibility, authority, and accountability which will without doubt continue to hamper efforts until and unless corrected by statute.

To correct this imbalance, I believe that elevating the GEC and it role of leading, coordinating, and synchronizing U.S. government efforts in the information environment to something similar to what the Office of National Intelligence does for the intelligence community would bring the appropriate alignment of responsibility, authority, and accountability while minimizing significant bureaucratic tension and cost.

Such an elevation in stature would enable the GEC to advocate for resourcing levels for the Interagency as well as drive a single information strategy and bring discipline to the whole of government efforts. I know firsthand that many talented people in government are working

these issues thoughtfully and diligently; unfortunately, they are not always working in unison because they are answering to different leaders with different priorities.

The Limitations of Truth and Bureaucracy

It is not unreasonable to think that the U.S. will always be at some disadvantage against our adversaries in the information environment. We are a nation of laws where truth and ethics are expected, and rightly so. Our enemies, on the contrary, are not constrained by ethics, the truth, or even the law. Our adversaries, both state and non-state actors, can and will continue to bombard all forms of communication with their messages in attempts to influence public perception, create doubt of our actions or intentions, and recruit people to their cause. We must ensure that we organize U.S. government efforts in such a manner that maximize desired outcomes through discipline, agility, and innovation.

When using the terms agility and innovation, the U.S. government is generally not the first thing to come to mind. This is especially true in the information environment as anyone who has served in government can attest. For example, it remains difficult to introduce new social media analytic tools and forensic tools onto government IT systems because of lengthy and highly complicated compliance processes. Although these tools are crucial to understanding the social media landscape and are required to ensure the U.S. efforts are hitting the right audience with the right message at the right time, we are often hampered by bureaucratic hurdles and outdated systems. Analytic tools are advancing as fast as the information environment itself and any lag in implementation can have a devastating effect.

To be clear, these tools cost money and it takes significant resources to train on these ever-advancing capabilities. While budgets for U.S. government information warfare and counter-propaganda efforts have increased significantly in recent years, they still pale in comparison to the resources applied to kinetic efforts. As single kinetic strike against a high value terrorist can tally into the hundreds of millions of dollars when conducted outside the area of active armed hostilities (when adding intelligence efforts before or after the strike) and in many cases, only have short term affects. While many obstacles can be overcome by new authorities and clarification on lines of authority, we must be clear that, simply put, more investment is also required.

Even when fully resourced and masterfully executed, information warfare and counter-propaganda efforts contain a high element of risk. While bureaucracy in government is necessary to standardize routine tasks, it cannot be left to control the totality of our efforts in the information environment. The bureaucratic standard operating procedure strives to reduce risk to almost zero which, while appropriate in certain circumstances, is not effective in the information space. A failure to accept a reasonable degree of risk can ultimately lead to diluted messaging efforts and result in missing the correct audience with an effective message that shifts their thought and/or behavior to our desired end state. To be successful in this fight we

must learn to accept a higher level of risk and accept the fact that sometimes we are just going to get it wrong despite our best efforts. When we do get it wrong, we must learn, adapt, and iterate our message rapidly to be relevant and effective.

In Conclusion

I applaud Congress as whole, and especially the Armed Services Committees of both chambers, for its leadership in seeking to address the urgent threats of disinformation and propaganda campaigns from state and non-state actors. Indeed, Congress has driven the Executive Branch to make real progress. That said, much more still needs to be done in order to even catch up with our adversaries, let alone effectively compete against them.

Michael D. Lumpkin
Phone: 202.679.4804
Email: warlordfrog@gmail.com

WORK EXPERIENCE

Leidos Health **12/17 - Present**
Reston, VA

Vice President for Human Performance and Behavioral Health
Designs and implements performance programs focused on optimizing human performance. Manages the daily operations and P&L (profit and loss) of this emerging health sector.

Neptune
Washington, DC **3/17 - 12/17**

Principal
Conducts research and consulting in the fields of defense, finance and healthcare focused on providing our clients access to highly regulated federal markets.

Department of State **1/16 – 1/17**
Washington, DC

Special Envoy/Coordinator for the Global Engagement Center
Served as the leader and manager of the new effort to combat the online messaging of terrorist groups such as the Islamic State of Iraq and Syria (ISIS).

Specific accomplishments include:

- Hand selected to design, build, and lead this organization.
- Designed social media strategies that leveraged private industry social media companies to maximize their capabilities while minimizing the cost to US taxpayers.
- Built an innovative and agile capability that fully leveraged cutting edge data analytic tools to ensure the right message was received by the right audience at the right time.

Department of Defense, Pentagon **12/13 – 1/16**
Washington, DC

Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (SO/LIC)
Nominated by President Obama and confirmed by the U.S. Senate to serve as the principal civilian advisor to the Secretary of Defense on special operations and low-intensity conflict matters to include oversight of policy and resources. These core tasks include counterterrorism; unconventional warfare; direct action; special reconnaissance; foreign internal defense; civil affairs, information and psychological operations; and counterproliferation of WMD. In addition to policy oversight for special operations and stability operations capabilities, provided policy oversight for strategic capabilities and force transformation and resources. This includes oversight of capability development to include general-purpose forces and the Department's support of counter narcotics activities. After the Secretary and Deputy Secretary, served as the principal official charged with oversight over all warfighting capabilities within the senior civilian management of the Department of Defense.

Specific accomplishments include:

- Simultaneously served as Acting Under Secretary for Policy.
- Led the Department's Task Force that oversaw the eradication of Ebola in Liberia. Sought and received emergency $1 billion dollar congressional reprogramming effort to support this effort.
- Oversaw DoD's efforts to return Sergeant Bowe Bergdahl to US control from the Taliban after five years of confinement.
- Restructured DoD's Prisoner of War (POW) and Missing in Action (MIA) accounting community to be more responsive to families and their loved ones.
- Provided oversight of U.S. Special Operations Command's (USSOCOM) $10.6 billion dollar budget.
- Championed and sought congressional support and budgets that led to the growth of the USSOCOM.
- Awarded the Distinguished Public Service Medal

Department of Defense, Pentagon **5/13 – 12/13**
Washington, DC

Special Assistant to the Secretary of Defense
Recruited by Secretary Chuck Hagel to serve as advisor to Secretary of Defense on personnel and readiness issues of the armed services. Specific emphasis on the redesigning the military's electronic health records ensuring capability with the Department of Veterans Affairs and restructuring Departmental oversight and accountability in combatting sexual assault in the military.

- Awarded the Distinguished Public Service Medal

Industrial Security Alliance Partners, USA **5/12 – 4/13**
Chief Executive Officer
Responsible for all aspects of management of Industrial Security Alliance Partners (ISAP) holding company, its wholly owned subsidiaries, and relationships with key partners. Led and managed the profit and loss aspects of six companies focused on the national security sector. ISAP product offerings include innovative energy solutions, tactical equipment, and tactical training facilities. Served as a voting member of the Board of Directors and interacted daily with shareholders and customers on a daily basis.

Department of Defense, Pentagon **5/12 – 4/13**
Washington, DC

Consultant to the Secretary of Defense
Served as on-call, unpaid consultant to the Secretary of Defense.

Department of Defense, Pentagon **4/11 – 5/12**
Washington, DC

Principal Deputy Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (SO/LIC)
In addition to duties of Principal Deputy Assistant Secretary served as Assistant Secretary from April until December of 2011. Served as the principal civilian advisor to the Secretary of Defense on special operations and low-intensity conflict matters to include oversight of policy and resources. These core tasks include counterterrorism; unconventional warfare; direct action; special reconnaissance; foreign internal defense; civil affairs, information and psychological operations; and counterproliferation of WMD. In addition to policy oversight for special operations and stability operations capabilities, provided policy oversight for strategic capabilities and force transformation and resources. This includes oversight of capability development to include general-purpose forces and the Department's support of counter narcotics activities. After the Secretary and Deputy Secretary, served as the principal official charged with oversight over all warfighting capabilities within the senior management of the Department of Defense.

Specific accomplishments include:

- Served as both Principal Deputy and Acting Assistant Secretary for much of incumbency.
- Coordinated USSOCOM policies and objectives with Interagency counterparts as a member of the Counter Terrorism Board of Directors.
- Reorganized oversight of USSOCOM, ensuring availability of the special operations capacity critical to the National Security Strategy. The reorganization

significantly enhanced the Department's oversight of USSOCOM's $10.4 billion-dollar budget and 66,000-member force.

- Effectively advocated for both critical special operations capabilities and the building partnership capacity mission which resulted in programmatic growth in both areas despite significant budget reductions within the Department over the next ten years.
- Designed and oversaw the implementation of the Department's Counter Threat Finance mission, including the development of the Department of Defense Counter Threat Finance cells in Iraq, Afghanistan, and at the Combatant Commands, which has significantly degraded terrorist capabilities.
- Restructured the Department's strategy for supporting interagency counternarcotic efforts. Effectively designed a threat based model that realized significant efficiencies and cost savings in this $1.48 billion-dollar program while enhancing support.
- Provided oversight of sensitive special operations which significantly weakened al-Qaida and its affiliates resolving threats to the homeland abroad.
- Twice awarded Outstanding Public Service Medal.

Department of Veterans Affairs, Washington, DC **8/10 – 4/11**

Senior Advisor to the Secretary/Deputy Chief of Staff for Operations
Served as Senior Advisor to the Secretary of Veterans Affairs on issues specific to Veteran healthcare and benefits. As the only Veteran of either Iraq or Afghanistan in the Office of the Secretary, provided insight on those concerns specific to the current generation of Veterans. As Deputy Chief of Staff for Operations, oversaw the Department's operations on behalf of the Secretary and served as principal interface with the Under Secretaries of Health, Benefits, and National Cemeteries.

Specific accomplishments include:

- Served as interlocutor between the Department, White House, Department of Defense, Veteran Service Organizations, and the Congress in the successful development and implementation of a comprehensive caregiver support program for post 9/11 Veterans. Developed supporting budgeting and spend plans for $1.5 billion dollars over 5-year implementation based on new legislation. This program has been universally praised by its participants and all stakeholders.
- Restructured the Department's Office of Small and Disadvantaged Business Utilization (OSDBU) to ensure it was effectively servicing Veterans through rapid status verification. The verification process was streamlined which significantly reduced processing time and improved accuracy.
- Coordinated execution within the Department for the Secretary's vision to end Veteran's homelessness by 2015.

ATI **4/08 – 8/10**

Executive Director of Business Development

Responsible for both business generation and overall operations of this midsized defense business focused on tailored logistics and complex distribution.

Department of the Navy **10/86 – 9/07**
Naval Officer

- US Navy SEAL who held every leadership position from Platoon Commander to Team Commanding Officer. Veteran of numerous campaigns and contingency operations around the world that included deployments to Afghanistan, Colombia, Iraq, Panama, Philippines, and Somalia. Served on active duty in the U.S. Navy for 21 years.

Unique assignments/specific accomplishments:

- USSOCOM Office of Legislative Affairs. Served as USSOCOM's liaison to Capitol Hill. Represented USSOCOM's equities to both House and Senate authorizers and appropriators.
- Deputy Commander, Joint Special Operations Task Force – Arabian Peninsula. Oversaw the daily operations of 2,000 special operators and supporting personnel in 40 locations throughout Iraq.
- Commanding Officer of Naval Small Craft and Technical Training School
- Qualified as both US Navy SEAL and Surface Warfare Officer.
- Received over 40 awards and citations for superior performance both on and off the battlefield.

Highest Education
Naval Postgraduate School **1995**
Master of Arts, National Security Affairs

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MARCH 21, 2018

QUESTION SUBMITTED BY MR. LANGEVIN

Mr. LANGEVIN. The internet has significantly changed propaganda delivery. Social media platforms have lowered the cost of entry, while simultaneously increasing targeting fidelity and output. These activities are not necessarily cyber operations but do occur through cyberspace. The elevation of cyberspace as a domain of warfare caused us to rewrite U.S. doctrine, separating cyber operations from information operations. Our adversaries do not make this distinction. Instead of cyberspace, Russia refers to the information space. How do you feel the separation of cyber and IO has affected capability integration and effectiveness?

General BREEDLOVE. [The information was not available at the time of printing.]

QUESTION SUBMITTED BY MR. SCOTT

Mr. SCOTT. Declassified CIA assessments from 1983 detail specific Russian active measures related to the previous generations nuclear modernization and missile defense programs. For example, one report stated: "their campaign covers a whole spectrum of activities—from overt efforts to create a fear of nuclear war to covert measures, including forgeries and disinformation."

General Breedlove, how much have Russian tactics changed from the Soviet days and adapted themselves to new technologies?

General BREEDLOVE. [The information was not available at the time of printing.]

QUESTIONS SUBMITTED BY MR. BANKS

Mr. BANKS. Mr. Lumpkin, last week, General Mattis met with senior U.S. and Afghan officials to discuss the military campaign addressing the Taliban threat. Despite the promising intentions of the meeting and the note that the Taliban "may" be willing to pursue negotiations, without the entire Taliban leadership on board or firmly engaged, these meetings continue to yield little in terms of measurable success.

Hon. Lumpkin, how can the U.S. and coalition forces minimize Taliban influence on the domestic population so we accomplish the goal of winning the people's hearts, minds, trust and commitment to democracy?

What does this influence look like? Is it only brute force, extortion, coercion, and intimidation or are there sneakier, softer forms?

Despite the U.S. air campaign ramping up, are there ways to minimize Taliban influence that don't endanger American lives?

Do you suspect any adversarial or competitive states (e.g. Russia, China, Iran) influencing against us in the war on terror in this area of responsibility? Please detail, if so.

Mr. LUMPKIN. *How can the U.S. and coalition forces minimize Taliban influence on the domestic population so we accomplish the goal of winning the people's hearts, minds, trust and commitment to democracy?*

The lack of infrastructure and strong central government in Afghanistan makes technical influence methods largely ineffective. Technical influence delivery methods to include television, radio, and social media are not viable methods of influence when much of the population neither has access nor the infrastructure to receive such means of communication. Highly successful influence operations cannot be achieved in Afghanistan without a much larger commitment by U.S. and Coalition forces operating with extended horizons.

What does influence look like? Is it only brute force, extortion, coercion, and intimidation or are there sneakier, softer forms?

Influence is dependent on the targeted audience. Variables like audience culture, size, and available infrastructure must be taken into consideration. Many variables must be factored into creating a discrete program to achieve very specific goals against a targeted audience. The most effective methods of influence do not consist of brute force, extortion, coercion, and intimidation. Subtle influence methods where

the audience does not overtly recognize that they are targeted are the most effective methods.

Despite the U.S. air campaign ramping up, are there ways to minimize Taliban influence that don't endanger American lives?

No. American lives will be endangered as long as we continue operations in Afghanistan. It is the nature of military operations during open hostilities or low intensity conflict.

Do you suspect any adversarial or competitive states (e.g. Russia, China, Iran) influencing against us in the war on terror to this area of responsibility? Please detail, if so.

Indeed there are adversarial or competitive States that are actively influencing both the Taliban and general population in Afghanistan. Afghanistan's neighboring States are actively conducting direct and indirect influence operations in the country. This key influencing neighbors of Afghanistan are Iran and Pakistan. Each is conducting influence operation to achieve their own specific goals.

Mr. BANKS. Mr. Lumpkin, thank you for your service as well as for your frank and hard-hitting testimony. I agree that our adversaries have taken advantage of the U.S. rule of law and order with their disregard for any adherence to international norms of conduct. Your assessment of the Global Engagement Center (GEC) is helpful as well.

How do you envision a GEC with the right authorities and capabilities, works within the law, and is still nimble enough to outpace strategic competitors, but also doesn't create another bureaucracy?

While the Director of National Intelligence has a number of authorities and duties as the principal intelligence advisor to the President with a well-defined intelligence community, the stakeholders within the "information environment" are not as well defined across the U.S. Government. How well defined the stakeholders in the "information environment" in law? If they are not well-defined, what is the remedy?

How do you envision this future GEC working in conjunction with the National Security Council and Staff? How would you delineate responsibilities between the two?

Mr. LUMPKIN. *How do you envision a GEC with right authorities an capabilities, works within the law, and is still nimble enough to outpace strategic competitors, but also doesn't create another bureaucracy?*

The GEC should be orchestrating the information activities in the federal government and not actually conducting information operations themselves. A narrow charter will limit bureaucratic growth and allow for agility. At the same time, Congress should be actively involved in providing strong and robust oversight to ensure that the GEC has the correct capabilities in the ever-evolving information environment.

While the Director of National Intelligence has a number of authorities and duties as the principal intelligence advisor to the President with a well-defined intelligence community, the stakeholders within the "information environment" are not well defined across the U.S. Government. How well defined are the stakeholders in the "information environment" in law? If they are not well defined, what is the remedy?

I strongly recommend Congress conduct an "information environment" review of both the oversight structure and laws surrounding the key elements to include Public Diplomacy, Public Affairs, and Information Operations. Each has unique laws and policies as well oversight structure. The means of communication and influence have drastically evolved over the past twenty years but the laws and governance structure have failed to keep pace.

How do you envision this future GEC working in conjunction with the National Security Council and Staff? How would you delineate responsibilities between the two?

I believe the GEC Director should be both Senate confirmed and a member of the National Security Council. Like the Director of National Intelligence, this would provide a structure for open and full interoperability between the GEC and National Security Council.

○