S. HRG. 115–426

CYBER–ENABLED INFORMATION OPERATIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY

OF THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

April 27, 2017

Printed for the use of the Committee on Armed Services

Available via the World Wide Web: http://www.Govinfo.gov/

U.S. GOVERNMENT PUBLISHING OFFICE
34–175 PDF WASHINGTON : 2019

COMMITTEE ON ARMED SERVICES

JOHN MCCAIN, Arizona, *Chairman*

JAMES M. INHOFE, Oklahoma	JACK REED, Rhode Island
ROGER F. WICKER, Mississippi	BILL NELSON, Florida
DEB FISCHER, Nebraska	CLAIRE MCCASKILL, Missouri
TOM COTTON, Arkansas	JEANNE SHAHEEN, New Hampshire
MIKE ROUNDS, South Dakota	KIRSTEN E. GILLIBRAND, New York
JONI ERNST, Iowa	RICHARD BLUMENTHAL, Connecticut
THOM TILLIS, North Carolina	JOE DONNELLY, Indiana
DAN SULLIVAN, Alaska	MAZIE K. HIRONO, Hawaii
DAVID PERDUE, Georgia	TIM KAINE, Virginia
TED CRUZ, Texas	ANGUS S. KING, JR., Maine
LINDSEY GRAHAM, South Carolina	MARTIN HEINRICH, New Mexico
BEN SASSE, Nebraska	ELIZABETH WARREN, Massachusetts
LUTHER STRANGE, Alabama	GARY C. PETERS, Michigan

CHRISTIAN D. BROSE, *Staff Director*
ELIZABETH L. KING, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY

MIKE ROUNDS, South Dakota, *Chairman*

DEB FISCHER, Nebraska	BILL NELSON, Florida
DAVID PERDUE, Georgia	CLAIRE MCCASKILL, Missouri
LINDSEY GRAHAM, South Carolina	KIRSTEN E. GILLIBRAND, New York
BEN SASSE, Nebraska	RICHARD BLUMENTHAL, Connecticut

CONTENTS

APRIL 27, 2017

	Page
CYBER-ENABLED INFORMATION OPERATIONS	1
Inglis, John C., Former Deputy Director, National Security Agency	4
Lumpkin, Honorable Michael D., Principal at Neptune Computer Incorporated and Former Acting Under Secretary of Defense for Policy	8
Waltzman, Rand, Ph.D., Senior Information Scientist, Rand Corporation	12
Watts, Clint, Robert A. Fox Fellow, Foreign Policy Research Institute	19

CYBER–ENABLED INFORMATION OPERATIONS

THURSDAY, APRIL 27, 2017

U.S. SENATE,
SUBCOMMITTEE
ON CYBERSECURITY,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:33 p.m., in Room SR–222, Russell Senate Office Building, Senator Mike Rounds (chairman of the subcommittee) presiding.

Present: Senators Rounds, Fischer, Nelson, McCaskill, Gillibrand, and Blumenthal.

OPENING STATEMENT OF SENATOR MIKE ROUNDS

Senator ROUNDS. Good afternoon. We will call this meeting to order. The Cybersecurity Subcommittee meets today to receive testimony on cyber-enabled information operations, to include the gathering and dissemination of information in the cyber domain.

We are fortunate to be joined this afternoon by an expert panel of witnesses: Chris Inglis, former Deputy Director of the National Security Agency; Michael Lumpkin, principal at Neptune Computer Incorporated and the former Acting Under Secretary of Defense for Policy; Rand Waltzman, senior information scientist at RAND Corporation; and Clint Watts, the Robert A. Fox Fellow at the Foreign Policy Research Institute.

At the conclusion of my remarks and those of Senator Nelson, we will hear briefly from each of our witnesses. I ask our witnesses to limit their opening statements to 5 minutes, in order to provide maximum time for member questions. We will be accepting your entire statements for the record.

The subcommittee has conducted two classified briefings on cyber threats and deterrence of those threats. The purpose of those briefings was to help our new subcommittee analyze the current situation, to include the threat as well as our own strengths and weaknesses.

The briefings included discussion of the report of the Defense Science Board's Task Force on Cyber Deterrence. Today, in our first open forum, we will further discuss threat capabilities, specifically those of Russia, to use new tools to obtain and disseminate information in this new domain of conflict.

I would also note that we will follow the 5-minute rule and the early bird rule today as we move forward.

Russian information operations, like those we experienced during the 2016 election and currently ongoing in Europe, are not new.

Many nation-states, in one form or another, seek to shape outcomes, whether they be elections or public opinion. They do this to enhance their national security advantage. In particular, the Soviet Union conducted decades of disinformation operations against the United States and our allies.

However, today's cyber and other disinformation-related tools have enabled Russia to achieve operational capabilities unimaginable to its Soviet forbearer.

Our hearing today is not intended to debate the outcome of the 2016 election, which experts agree was not undermined by any cyberattacks on our voting infrastructure or the counting of ballots. But the purpose of today's hearing is to learn from that experience and other such experiences in order to assess how information operations are enhanced in terms of the reach, speed, agility, and precision, and impact through cyberspace.

Ultimately, we will continue to struggle with cyber-enhanced information operation campaigns until we address the policy and strategy deficiencies that undermine our overall cyber posture.

In other words, my hope is that this hearing will be forward-, not backward-looking, and help lay the foundation for the legislation and oversight necessary to address this national security threat.

Disinformation and fake news pose a unique national security challenge for any society that values freedom of speech and a free press. Our adversaries aim to leverage our distaste for censorship against us to delegitimize our democracy, influence our public discourse, and ultimately undermine our national security and confidence. It is imperative that we use our experience with the 2016 election to create the defenses necessary to detect and respond to future efforts.

We look to our witnesses to help us better understand the threats we face and develop the tools we need to address it.

Just last month, we heard from the Defense Science Board about the urgent need for cyber deterrence. According to the Board's findings, for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructure. Our ability to defend against cyber-enabled information operations will also likely require an element of deterrence and demonstrating that actions will have consequences.

With that in mind, we look to our witnesses to help us better understand the challenges that cyber-enabled information operations will pose for us in the future and what they believe will be required to counter this threat.

Information operations are not new and have been used in one form or another in nearly every conflict throughout history. Cyberspace has and will continue to enhance the scope and reach of these campaigns. Our ability to develop a strategy to deter and repel cyber-enabled operations is critical. Our citizens' confidence in our democratic process depends on it.

As we begin our first open hearing, I want to express my gratitude for the opportunity to serve with our ranking member, Senator Bill Nelson. In addition to his great service to our Nation, Senator Nelson brings a wealth of knowledge and experience that I

know all members of our subcommittee will look to in the days ahead.

Senator Nelson?

STATEMENT OF SENATOR BILL NELSON

Senator NELSON. Thank you, Mr. Chairman, and thank you for your very gracious remarks.

Thank you as we proceed on trying to piece together a new threat, one that we have seen employed against our country and our basic foundations of our country. Because even though information warfare has been used for years and years, we know now, as a result of the Internet, there are all new opportunities for mischief, because we have seen, at a small cost, both in terms of people and money, a regime like Putin's regime can directly access the people of the United States, bypassing traditional media filters. It is possible to weaponize information to accomplish their particular objectives.

As we learned last year, even our private and sensitive communications, such as the email in a political campaign, can be stolen through cyber hacking and then released through established media. In this way, modern technologies and tools—social media platforms, cyber hacking to steal information—can therefore create armies of robot computers and the so-called big data analytics powered by artificial intelligence, all of that can amplify the speed, scale, agility, and precise targeting of information operations beyond what was imaginable back in the heyday of the Cold War, when there were two big superpowers and we were at each other with our information campaigns. This is a whole new magnitude greater.

These tools and operations support are enhanced by the more traditional elements, such as the multimedia Russia Today network and Sputnik. Those two spread disinformation and propaganda while trying to appear as objective news sources.

As the testimony of this committee has already heard in prior hearings, and as the prepared statements of our distinguished panel of witnesses today confirm, our government and our society remain ill-prepared to detect and counter this powerful new form of information warfare or to deter it through the threat of our own offensive information operations.

Our witnesses, however, today will explain that it is, indeed, possible to apply the same technologies used by the adversaries against them to fight back against their aggression.

But harnessing and applying these technologies ourselves effectively, both defensively and offensively, will require significant changes to the way we are organizing tasks both inside the Department of Defense and other agencies.

Moreover, success also requires a deep partnership between the public and the technology companies who have built and operate the networks and platforms where this conflict is playing out.

This is a tremendous challenge that we face today. I thank you, Mr. Chairman, for calling this hearing.

Senator ROUNDS. Thank you, Senator Nelson.

At this time, we would like to begin with 5-minute opening statements.

If you would prefer, Mr. Inglis, you may begin.

STATEMENT OF JOHN C. INGLIS, FORMER DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

Mr. INGLIS. Chairman Rounds, Ranking Member Nelson, members of the committee, thanks very much for the opportunity to appear here today.

I will be very brief. I have submitted a written statement for the record, but I would like to make, upfront, four quick points.

First, on the true nature of cyberspace, as we consider what happens in this domain, which I believe is, in fact, a new domain extended from the old domains, you can think of it as a noun. That noun, in my view, would be that it is the meld of technology and people and the procedures that bind to the two. If we try to solve just one of those three pillars, we will find out that the other two will defeat us.

If you think about the verb, what is happening in that space is massive connectivity, fading borders, and an exponential increase in the ratio of data to information. There is a lot more data, but that doesn't mean that we know a lot more, that we have a lot more information.

The second point, on the trends that compound the importance of cyberspace, there are, in my view, four trends that essentially side by side with this onrush of technology make a difference to our deliberations here today.

The first is that there is a new geography. It is not independent of cyberspace. But companies, individuals, begin to think about their opportunities, their aspirations based upon a geography that is not physical anymore. It is based upon opportunities without regard to physical borders or the jurisdictions that typically go hand in glove with those physical borders.

Second, there is a new means for organizing people. People organize by ideology as much or more as by proximity. In the physical world, that gives rise to a lone wolf terrorist. In the cyber world, that gives rise to people who you think are aligned with your values but are not necessarily because they reach across the borders that you can see.

Three, there are disparities that continue to exist in the world. That is no great surprise. It has been with us since the dawn of time. But those disparities are increasingly reconciled in and through cyberspace. Whether by collaboration or competition or conflict, disparities in wealth and treasure, disparities in religious respects, disparities in all manner of things, cyber is the new venue for reconciliation.

Finally, not independent of that, geopolitical tension continues to exist. It too is increasingly reconciled in and through cyberspace.

Summing up those four trends, they tend to reduce the influence of traditional institutions—nation-states—by defusing roles, fading borders, and flooding us with data as opposed to information. But I would conclude nation-states are not dead yet.

The third major point that I would make is that it is increasingly important to consider the consequences of the scope, scale, and use of cyberspace.

My colleague, Dr. Waltzman, submitted a written record that talks about three levels of cyberspace. I will kind of take some liberties with that, but the foundation of that might be that you talk about the literal kind of infrastructure in that space, possibly the data. Just above that, you think then about what that content means. Just above that is the confidence that comes from having a reliance on those.

I kind of talk about those because we need to be clear about our terms. I was very much appreciative of Chairman Rounds' opening statement where he used the term information warfare as discrete from cyber warfare. Cyber warfare, in my view, is not a standalone entity. It is something that has to be a component of the larger state of war that exists between two entities.

When you talk about information warfare, it is at the third level. It is at that topmost stack. It is not necessarily comprised of an exchange of tools or an exchange of literal warfare. It is, in fact, a conflict of ideas. Some of those ideas we may prefer. Some of those ideas we may not. But we have to talk about those as distinct entities.

My final point would be that the issue before us is both about defending then cyberspace and also about defending the critical processes that depend upon our confidence in cyberspace. I would leave us with perhaps some things to think about in terms of what the attributes of a solution might look like.

We should remember that there are no strategic capabilities, only capabilities that are employed in the execution of strategic aims. We need to begin with the declaration of what those strategic aims are. We need to communicate them fully, faithfully, and in a collaborative manner.

We need to employ all instruments of power in a collaborative fashion. What we seek is not the proper sequencing of these instruments of power but a concurrent application of those instruments of power.

We need to stop reacting well and thinking that we, therefore, have done good, and start to drive and perhaps lead in this space, and at least anticipate well or track well.

Finally, as Ranking Member Nelson indicated, we can use the techniques that have been used against us, but we should never compromise our values, and there is a distinct difference between those two.

Thank you.

[The prepared statement of Mr. Inglis follows:]

PREPARED STATEMENT BY CHRIS INGLIS

Thank you, Chairman Rounds, Ranking Member Nelson, and Members of the Committee. I am pleased to appear before you today to talk on the topic of cyber enabled information operations.

As the committee noted in its invitation, "information operations" have been conducted as a component of state and non-state operations for centuries but have recently taken on significantly greater import because of the leverage, speed, scope and scale afforded them by the technologies and trends attendant to the rise of the internet.

My comments today are derived from twenty-eight years of experience at the National Security Agency working both of its related but distinguished missions: the Information Assurance mission supporting the defense of critical information and networks, and the Signals Intelligence mission which generates foreign intelligence

needed to inform the Nation's defense. While I possess technical degrees in engineering and computer science, the majority of my career at the National Security Agency was spent in leadership positions, including seven and one half years' service as NSA's senior civilian and Deputy Director during the period 2006–2014. Since July 2014, I have also served on several Defense Science Board studies on the topic of cyber, and as a visiting professor of cyber studies at the United States Naval Academy, which has been developing and delivering cyber education for future Naval and Marine Corps officers for several years. While the views I will express are necessarily mine alone, I will draw from the sum of these experiences in these opening remarks and throughout the question and answer period.

The committee's invitation letter asked for perspectives on the changes in **"scale, speed, and precision [afforded] by modern cyber hacking capabilities, social media and large-scale data analytics" as well as views on "technical, organizational, and operational means needed to detect and counter these operations, including public-private collaboration and international efforts."**

I will address these in brief opening remarks and welcome the opportunity to discuss in greater detail during the hearing's question and answer session.

The revolution afforded by the internet over the past forty years is one fueled by innovations in technology and the private sector's ability to deliver that innovation at scale and with supporting infrastructure to billions of consumers in an increasingly global marketplace.

While technology revolution is the visible phenomenon, there are several trends that greatly influence the impact of technology on society at large. I describe three such trends here that, while not independent of technology, are distinct from it, even as they exacerbate its effects.

- The first is a new geography wherein people and organizations increasingly see the internet as a jurisdiction in its own right, a jurisdiction that transcends the physical limitations and legal jurisdictions once defined by physical geography alone. The effects of this phenomenon necessarily attenuate the influence of governments and other jurisdictions that are based on physical borders. That fact notwithstanding, the impact can be quite positive, as in the case where the allocation of goods and services are optimized on a global basis, smoothing out sources, flows, and consumption; or quite negative, wherein the challenges of reconciling legal jurisdiction and the inherent difficulty of cyber attribution conspire to increase the challenge of achieving reasonable enforcement of legal norms in and through cyberspace.
- The second is a new social order wherein people increasingly organize by ideology as much or more by physical proximity alone. As with the new geography, the impact of this can be perceived as good or bad. The sweep of democratic ideals across many nations in the 2011 Arab Spring was largely borne of this phenomenon. In a similar manner, radicalization of lone wolf terrorists who are inspired to acts of terror without ever meeting their mentors makes use of the same mechanism. Wikileaks too is borne of this phenomenon—a force in the world that knows no physical borders even while it has an increasing effect—sometimes favorable, sometimes not—on institutions whose jurisdictions are often constrained by them.
- Finally, there is the increasing propensity of private citizens, organizations and nation-states to see cyberspace as a means of collaborating, competing, or engaging in conflict—activities that in previous times would have played out across physical geography employing traditional instruments of personal, soft or hard power. As with the other trends I define here, this trend can have effects perceived as good or bad. More importantly, the ubiquitous nature of cyberspace has made it increasingly likely that cyberspace will serve as the preferred venue for reconciliation of perceived disparity(ies) in the world—whether those disparities are in wealth, knowledge, or national interest. Witness the denial of service attacks by Iran on US financial institutions in 2012–2013, the attack by North Korea on Sony pictures in 2014, and the information war conducted by Russia against the US election process(es) in 2016.

The role of cyberspace as an essential foundation for personal pursuits, commerce, delivery of services, and national security combined with its use as a new geography, an alternative means for social organization and as a venue for reconciliation all converge to yield the challenges we experience on an almost daily basis. But because the challenges result from far more than technology and other phenomena within cyberspace itself, any attempt to address these larger strategic challenges will need to consider and address more than cyberspace itself.

To be more concrete, cyberspace may be considered as the sum of technology, people and the procedures and practices that bind the two. Any attempt to improve the resilience and integrity of cyberspace and the strategic things that depend on it must necessarily address all three and must, to the maximum extent possible, be constructed to work across physical borders as much or more as within them.

- By way of practical example, an organization desiring to improve the resilience of its information technology enterprise would do well to spend as much time and energy defining roles, policies and procedures as on the firewalls and security tools intended to comprise a defensible architecture. A review of cyber breaches over time clearly shows that failures in these procedures and human error are the principal weakness(es) exploited by cyber criminals, nation-state actors, and hacktivists.
- While technology must play a role in reducing the probability and impact of human error, vulnerabilities attributable to the human element will never be removed.
- In the same vein, governments must acknowledge that the globally interconnected nature of information systems and look for ways to craft laws and rules that will not be rejected by neighboring jurisdictions at some physical border, resulting in balkanization of systems and commercial markets, resulting in market inefficiencies, reduced system performance and security seams.

Some thoughts on essential elements of a solution follow:

Given the convergence of technology, the actions of individuals, and the collective actions of private and nations-state organizations that takes place in and through cyberspace, a bias for collaboration and integration must underpin any solutions intended to improve collective resilience and reliability. This calls for active and real-time collaboration, not simply divisions of effort, between the private and public sectors.

Analogous to security strategies defined in and for the physical world, the most effective solutions for cyberspace will leverage the concurrent and mutually supporting actions of individual actors, the private sector, the public sector, and Government coalitions.

The private sector remains the predominant source of cyber innovation as well as the majority owner and operator of cyber infrastructure. The private sector must therefore be empowered and accountable within the limits of its knowledge and control to create defensible architectures and defend them. While the Cyber Security Act of 2015 made an important down payment on the ability of private sector organizations to share cyber threat information, greater attention should be given to increasing the incentives for private sector organizations to share and act on time-critical information in the defense of their data, infrastructure and businesses.

Government efforts must be biased towards the defense of all sectors, vice the defense of its own authorities and capabilities alone (an extension of the so-called "equities problem" that has traditionally focused on sharing information on inherent flaws in software and hardware). Government information regarding threats and threat actors must be shared with affected persons and parties at the earliest possible opportunity with a bias to preventing the spread of threats rather than explaining-in-arrears the source and attribution of already experienced threats.

The recent creation of the United Kingdom's National Cyber Security Centre (NCSC) represents a useful example of this approach. Comprised of about several hundred government experts from GCHQ (the UK's counterpart to the National Security Agency), subject matter experts from private sector organizations, and integrees from various civil and military UK Government organizations, the NCSC's charter is to effect near-real-time collaboration between the private and public sectors, with an emphasis on the exchange of heretofore classified information. The resulting bias is to share without precondition, treating information as sharable by default, vice by exception. While the processes internal to the NCSC are worth examining, the transformation of private-public model for collaboration is the bigger story.

Uniquely Government authorities to conduct intelligence operations, negotiate treaties, define incentives, and employ inherently governmental powers (criminal prosecution, financial sanctions, military action among them) must be employed as a complement to private sector efforts, not independent of them. A bias towards collective action by like-minded Nations will enable their respective private citizens and commercial organizations to optimize the conduct of their pursuits in and through cyberspace.

Whole-of-government approaches will, over time, define the various circumstances where cyber offense, an inherently military capability, should be considered and em-

ployed. In this vein, offensive military cyber capability must be considered as a viable element of cyber power, neither the most preferred or the tool of last resort. The extreme conservatism of the U.S. Government in its use of cyber offensive power in the past has not been met with similar restraint by its principal adversaries and has retarded the development of operational capacity needed to deter or counter ever more aggressive adversaries. That said, cyber offense should be viewed as an extension of, rather than an alternative to, cyber defense, most practicable when it rests on a solid foundation of defensible architectures and the vigorous defense of those architectures.

While uniquely challenging, the deterrence of adversary misbehavior in cyberspace can be significantly improved. Improved resilience and vigorous defense of enterprise infrastructure will aid in deterrence by denial. Improved attribution and vigorous pursuit of adversaries who violate defined norms will aid in deterrence by cost imposition. Collaboration across private/public and international boundaries will improve yields in this arena.

Most important of all, it should be remembered that no capability, across the private or public sector, is inherently tactical or strategic. Strategic objectives set the stage for strategy. Capabilities and tactics only have meaning within that broader context.

To that end, the actions taken by Russia in 2016 against various facets of the American election system must be considered in the context of Russian objectives and strategy. When viewed as such, Russian actions were neither episodic nor tactical in scope or scale. The lesson for us about the role of strategy and proactive campaigns in identifying and harnessing diverse actions to a coherent end-purpose is clear. While we must not compromise our values through the use of particular tactics against potential or presumed adversaries, simply responding to adversary initiative(s) is a recipe for failure in the long-term.

We must define and hone our strategic objectives. Strategy must then allocate those objectives to the various instruments of power available to us. Our efforts will be most effective when reinforced by alliances and when fueled by the cross-leveraging effects yielded by the concurrent application of individual, private sector, public sector power where offense and defense complement rather than trade one another.

Finally, in as much as I describe a mandate for government action in this space, I think government action must be:

- Fully informed by the various interests government is formed to represent;
- Focused on ensuring the various freedoms and rights of individual citizens while also maintaining collective security;

and

- Mindful that the engine of innovation and delivery is almost exclusively found in the private sector.

To be clear, I do see a role for government both in facilitating the creation of an enduring, values based, framework that will drive technology and attendant procedures to serve society's interests, and in reconciling that framework to-and-with like-minded Nations in the world.

Conversely, I believe government's failure to serve in this role will effectively defer leadership to a combination of market forces and the preferences of other nation-states which will drive, unopposed, solutions that we are likely to find far less acceptable.

In that spirit, I applaud the initiative and further work of this committee in taking up the matter and working through these difficult issues.

I look forward to your questions.

Senator ROUNDS. Thank you, Mr. Inglis.

Mr. Lumpkin, would you care to begin?

STATEMENT OF HONORABLE MICHAEL D. LUMPKIN, PRINCIPAL AT NEPTUNE COMPUTER INCORPORATED AND FORMER ACTING UNDER SECRETARY OF DEFENSE FOR POLICY

Mr. LUMPKIN. Chairman Rounds, Ranking Member Nelson, distinguished members of the committee, thank you for the opportunity to be before you today.

I trust my experience as a career special operations officer, Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, and as coordinator and director of the Global Engagement Center will be helpful today, along with my panel members here, in giving perspective on the current status of the U.S. Government strategy, capabilities, and direction in informational warfare and counterpropaganda.

The previous administration and the 114th Congress demonstrated clear commitment to this issue. This is evidenced by President Obama's Executive Order 13721, which established the Global Engagement Center and the 2017 National Defense Authorization Act, which expanded that Center's mission.

The 2017 NDAA [National Defense Authorization Act] expanded the GEC's [Global Engagement Center] mandate to include counter-state propaganda and disinformation efforts well beyond the original charter, which limited it to being focused on countering terrorist propaganda.

This is a big step in the right direction, but the sobering fact is that we are still far from where we need to be to successfully operate and to have influence in the modern information environment.

Since the end of the Cold War with the Soviet Union, which was arguably the last period in history when the United States successfully engaged in sustained information warfare and counter-state propaganda efforts, technology and how the world communicates has changed dramatically.

We now live in a hyperconnected world where the flow of information moves in real time. 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 the U.S. and foreign audiences at the same time via the same benefits.

To illustrate this fact, as this committee is aware, it was a 33-year-old IT consultant in Abbottabad, Pakistan, that first reported the United States military raid against Osama bin Laden in May of 2011 on Twitter. This happened as events were still unfolding on the ground and hours before the American people were officially notified by the President's address.

While the means and methods of communications have transformed significantly over the past decade, much of the U.S. Government's thinking on shaping and responding in the information environment has remained unchanged, to include how we manage U.S. Government information dissemination and how we respond to the information of our adversaries.

We are hamstrung by a myriad of reasons, to include lack of accountability and oversight, bureaucracy resulting in insufficient levels of resourcing, and an inability to absorb cutting-edge information and analytic tools, and access to highly skilled personnel. This while our adversaries are increasing their investment in the information environment while not being constrained by ethics, the law, or even the truth.

The good news is that we have good people working on this effort. The work force is committed and passionate and recognize why this is important and why we as a Nation need to get it right.

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

[The prepared statement of Mr. Lumpkin follows:]

PREPARED STATEMENT BY HONORABLE MICHAEL D. LUMPKIN

INTRODUCTION

Chairman Rounds, Ranking Member Nelson, and distinguished members of the Committee, thank you for this opportunity to address you today as a private citizen and in an individual capacity on the topic of *Information Operations.* 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 at the Department of State will be helpful in providing perspective on the current status of the U.S. Government's strategy, capabilities, and direction in information warfare and counter-propaganda. The previous Administration and the 114th Congress demonstrated a clear commitment to this issue, as evidenced by the President Obama's Executive Order 13721 which established the Global Engagement Center (GEC) and the 2017 National Defense Authorization Act (NDAA) that expanded the Center's mission. The 2017 NDAA expanded the GEC's mandate to include counter-state propaganda and disinformation efforts, well beyond its original charter which limited it to diminishing the influence of terrorist organizations such as the Islamic State of Iraq and Syria (ISIS) in the information domain. This is a big step in the right direction, but the sobering fact is that we are still far from where we ultimately need to be to successfully operate in the modern information environment.

That said, I am very pleased to be joined here today by former Deputy Director of the National Security Agency John Inglis, Dr. Rand Waltzman from the RAND Corporation, and Mr. Clint Watts from the Foreign Policy Research Institute. Collectively, I believe we are 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 United States successfully engaged in sustained information warfare and counter-state propaganda efforts, technology and how the world communicates has changed dramatically. We now live in a hyper-connected world where the flow of information moves in real time. 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. To illustrate this fact, as this Committee is aware, it was a 33-year-old IT consultant in Abbottabad, Pakistan that first reported the United States military raid against Osama bin Laden in May of 2011 on Twitter. This happened as events were still unfolding on the ground and hours before the American people were officially notified by the President of the United States' address.

While the means and methods of communication have transformed significantly over the past decade, much of the U.S. Government thinking on shaping and responding in the information environment has remained unchanged, to include how we manage U.S. Government information dissemination and how we respond to the information of our adversaries. We are hamstrung for a myriad of reasons to include: lack of accountability and oversight, bureaucracy resulting in insufficient levels of resourcing and inability to absorb cutting-edge information and analytic tools, and access to highly skilled personnel.

LACK OF ACCOUNTABILITY AND OVERSIGHT

To date, there is not a single individual in the U.S. Government below the President of the United States who is responsible and capable of managing U.S. information dissemination and how we address our adversaries in the information environment. 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, but it fell short in elevating it to a position where it could fully execute its mission. The GEC operates at the Assistant Secretary level and lacks the 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 several disparate organizations at the Department of Defense, to say nothing of the other departments and agencies that have a stake in this fight.

Furthermore, although the GEC is directed by law with the mission to lead the Interagency, its role is reduced to simply a "suggesting" function. It is then up to the respective agency whether to comply. This misalignment of responsibility, authority, and accountability will without doubt continue to hamper the efforts of the GEC until it is ultimately corrected by statute.

Before his departure as the Director of National Intelligence, Jim Clapper told this Congress that the United States needs to resurrect the old U.S. Information Agency (USIA) and put it on steroids. While I agree with DNI Clapper that we need to increase our focus and management of the information environment, I do not believe that resurrecting the USIA in its previous form will allow the U.S. Government to be relevant in the ever-changing information landscape. While the USIA had many positives, there were also many challenges which ultimately resulted in its disestablishment. That said, DNI Clapper was figuratively closer to a solution than even he may have thought. Elevating the GEC and its role of leading, coordinating, and synchronizing U.S. Government efforts to something similar to what the Office of the Director of National Intelligence does with intelligence would bring alignment between responsibility, authority, and accountability while minimizing significant bureaucratic tension and cost.

Such an elevation in stature would allow the GEC to advocate for resourcing levels for the Interagency as well as drive a single information strategy and bring discipline to the U.S. Government efforts. Many talented people in government are working this issue thoughtfully and diligently, unfortunately they are not always working in unison because they are answering to different leaders with different priorities.

THE LIMITATIONS OF THE TRUTH AND BUREAUCRACY

It is not unreasonable to think that the United States 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 the law. Our adversaries, both State and non-State actors, can and will bombard all forms of communications to include traditional media and social media with their messages to influence, create doubt of our actions or intentions, and even recruit people to their cause. We must ensure that we organize our 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 that to comes to mind. This also holds true in the information environment. For example, it remains difficult to introduce new social media analytic and forensic tools onto government IT systems because of lengthy and highly complicated compliance processes. These tools are critical 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 that influences thought or behavior. Analytic tools are advancing as fast as the information environment itself and time delays in implementation can have a devastating effect.

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, they still pale to the resources applied to kinetic efforts. A single kinetic strike against a single high value terrorist can tally into the hundreds of millions of dollars when conducted outside an area of active armed hostilities (when adding intelligence preparation before and after the strike) and in many cases, only have short term affects. At the same time the GEC funding in fiscal year 2017 is below $40 million. Again, please keep in mind that this is a significant increase from the GEC fiscal year 2015 budget of $5.6 million. We are making progress just not fast enough to turn the tide in our favor any time soon as many of our adversaries are putting significantly more resources into information operations than we are.

Even when fully resourced and masterfully executed, information warfare and counter-propaganda efforts can 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 can ultimately lead to diluted messaging efforts that can result in missing the right audience with an effective message that shifts their thought and behavior to our desired end state. To be successful 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 messaging rapidly to be relevant and effective.

ACCESS TO TRAINED PERSONNEL

As mentioned previously, there are some talented people in government working the information environment challenge. There are, however, just not enough of them nor are they always able to keep up with the technological advances in this arena. Some success has been realized in using the Section 3161 hiring authority granted to the GEC by Executive Order 13721. This authority allows the GEC to hire limited term/limited scope employees directly into government based on their skills and capabilities. This has provided the GEC access to experienced private sector talent that government service does not traditionally provide. Access to the talent of academia, Silicon Valley, and Madison Avenue now is possible for the GEC. Unfortunately, outside of the GEC, other federal departments and agencies do not have the ability to leverage the Section 3161 hiring authority to access top talent in the field.

IN CONCLUSION

Recognition of the importance of U.S. Government's role in the information environment continues to grow as exemplified by the creation and expansion of the GEC. Indeed, significant progress has made. It is imperative, however, that the government's efforts be fully coordinated and resourced to be responsive and adaptive. The information environment and our adversaries' actions will continue to evolve and our means and methods need to remain agile and innovative to stay relevant and effective in the emerging security environment.

Senator ROUNDS. Thank you, sir.

Dr. Waltzman, you may begin.

STATEMENT OF RAND WALTZMAN, Ph.D., SENIOR INFORMATION SCIENTIST, RAND CORPORATION

Dr. WALTZMAN. Chairman Rounds, Ranking Member Nelson, and distinguished members of the committee, I would also like to thank you for inviting me to testify today.

I would like to start out by telling you a story. In March 2006 in Iraq, one of our special forces battalions engaged a unit of the Jaish al-Mahdi death squads. In this engagement, our guys killed 16, captured 16, freed a badly beaten hostage, and destroyed a major weapons cache, and left the scene thinking this was a successful operation.

Unfortunately, there was one catch. By the time they got back to their base within 1 hour, the remnants of the Jaish al-Mahdi death squad had come in, cleaned the scene up, taken their fallen comrades, arranged them on prayer mats, and made it look—and took pictures with a mobile phone, pushed pictures out into the social media, onto the Internet, including press releases in English and Arabic, and claimed that those people were murdered in the middle of prayer unarmed. All of that was done before our guys got back to the base, just like that. It was amazing.

Now, it took the Army 3 days to respond to that, and those guys film everything they do. Not only did it take 3 days to respond, but an investigation ensued that kept those people benched for 30 days.

This turned out to be a major psychological defeat on what people thought was a successful kinetic operation.

The question you should be asking yourselves at this point, I hope, is, how did they manage to do this so fast? They did not plan on being killed. They do not plan on an engagement. Yet they managed.

Operations in the information environment are starting to play a dominant role in everything from politics to terrorism, to geopolitical warfare and even business, all things that are becoming increasingly dependent on the use of techniques of mass manipula-

tion. These operations are complicated by the fact that in the modern information environment, they occur at a speed and an extent previously unimaginable.

Traditional cybersecurity is all about defense of information infrastructure. Unfortunately, traditional cybersecurity is not going to help against these types of attacks. Something quite different is required. The problem requires a different approach and a different set of supporting technologies, which I will call, collectively, cognitive security.

To emphasize the difference, I would like you to consider a classical denial of service attack. In a classical denial of service attack, the object of the attack is to bring down a server. The way you do it is by generating massive amounts of content-free messages that simply overload the server's capability to function, and it dies.

Now, on the other hand, a cognitive denial of service attack works in quite a different way. As an example, I would like to bring out the Russian elections in 2011.

In December, there was going to be a demonstration planned by antigovernment forces, and they were going to use Twitter to organize the election using the hashtag Triumfalnaya, which was the name of the square. That was the word that people could use to find the tweets that contained the instructions.

Unfortunately, the pro-government forces found out about this and started to automatically generate at the rate of 10 tweets per second messages that were just filled with garbage, just all kinds of rubbish, which produced a cognitive overload on the people who were being organized.

Twitter did not shut it down because it did not violate Twitter's terms of services. It was not a denial of services attack in the traditional sense. Yet, it brought the thing to its knees and destroyed the operation.

To make cognitive security a reality and counter this growing threat in the information environment, I would like to suggest a strategy of two basic actions.

The first one is the establishment of a center of excellence in cognitive security. This would be a nonprofit, nonpartisan, nongovernmental organization devoted to research, development, and education in policies, technologies, and techniques of information operations. The center would not be operational but rather set research and development agendas, and provide education and distribution of technologies and service to any of the communities that it would serve.

The second is a study conducted by an organization, like the Office of Net Assessment, for example. This study would answer three fundamental questions. The first is, what are the laws and policies that currently make operations in the information environment difficult to impossible, including problems of authorities? Second, how can those laws and policies be updated to support the realities of the modern information environment? Third, what kind of organizational structure is needed to manage cognitive security?

For further details, I refer you to my written testimony.

Thank you.

[The prepared statement of Dr. Waltzman follows:]

PREPARED STATEMENT BY DR. RAND WALTZMAN [1], THE RAND CORPORATION [2]

Dimitry Kiselev, director general of Russia's state-controlled *Rossiya Segodnya* media conglomerate, has said: "Objectivity is a myth which is proposed and imposed on us." [3] Today, thanks to the Internet and social media, the manipulation of our perception of the world is taking place on previously unimaginable scales of time, space and intentionality. That, precisely, is the source of one of the greatest vulnerabilities we as individuals and as a society must learn to deal with. Today, many actors are exploiting these vulnerabilities. The situation is complicated by the increasingly rapid evolution of technology for producing and disseminating information. For example, over the past year we have seen a shift from the dominance of text and pictures in social media to recorded video, and even recorded video is being superseded by live video. As the technology evolves, so do the vulnerabilities. At the same time, the cost of the technology is steadily dropping, which allows more actors to enter the scene.

THE GENERAL THREAT

Traditionally, "information operations and warfare, also known as influence operations, includes the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent." [4] This definition is applicable in military as well as civilian contexts. Traditional techniques (e.g. print media, radio, movies, and television) have been extended to the cyber domain through the creation of the Internet and social media.

These technologies have resulted in a qualitatively new landscape of influence operations, persuasion, and, more generally, mass manipulation. The ability to influence is now effectively "democratized," since any individual or group can communicate and influence large numbers of others online. Second, this landscape is now significantly more quantifiable. Data can be used to measure the response of individuals as well as crowds to influence efforts. Finally, influence is also far more concealable. Users may be influenced by information provided to them by anonymous strangers, or even by the design of an interface. In general, the Internet and social media provide new ways of constructing realities for actors, audiences, and media. It fundamentally challenges the traditional news media's function as gatekeepers and agenda-setters. [5]

Interaction within the information environment is rapidly evolving, and old models are becoming irrelevant faster than we can develop new ones. The result is uncertainty that leaves us exposed to dangerous influences without proper defenses.

The information environment can be broadly characterized along both technical and psychosocial dimensions. Information environment security today (often referred to as cybersecurity) is primarily concerned with purely technical features—defenses against denial-of-service attacks, botnets, massive Intellectual Property thefts, and other attacks that typically take advantage of security vulnerabilities. This view is too narrow, however. For example, little attention has been paid to defending against incidents like the April 2013 Associated Press Twitter [6] hack in which a group hijacked the news agency's account to put out a message reading "Two explosions in the White House and Barack Obama is injured." This message, with the weight of the Associated Press behind it, caused a drop and recovery of roughly $136 billion in equity market value over a period of about five minutes. This attack exploited both technical (hijacking the account) and psychosocial (understanding market reaction) features of the information environment.

Another attack [7], exploiting purely psychosocial features, took place in India in September 2013. The incident began when a young Hindu girl complained to her family that she had been verbally abused by a Muslim boy. Her brother and cousin

---

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of the RAND Corporation or any of the sponsors of its research.

[2] The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

[3] Joshua Yaffa, "Dmitry Kiselev Is Redefining the Art of Russian Propaganda," New Republic, July 14, 2014.

[4] RAND Corporation, "Information Operations," web site, undated.

[5] Rand Waltzman, "The Weaponization of the Information Environment," American Foreign Policy Council Defense Technology Program Brief, September 2015a.

[6] Max Fisher, "Syrian Hackers Claim AP Hack That Tipped Stock Market by $136 Billion. Is It Terrorism," Washington Post, April 23, 2013.

[7] Mark Magnier, "Hindu Girl's Complaint Mushrooms into Deadly Indian Riots," Los Angeles Times, September 9, 2013.

reportedly went to pay the boy a visit and killed him. This spurred clashes between Hindu and Muslim communities. In an action designed to fan the flames of violence, somebody posted a gruesome video of two men being beaten to death, accompanied by a caption that identified the two men as Hindu and the mob as Muslim. Rumors spread like wildfire that the mob had murdered the girl's brother and cousin in retaliation over the telephone and social media. It took 13,000 Indian troops to put down the resulting violence. It turned out that while the video did show two men being beaten to death, it was not the men claimed in the caption; in fact, the incident had not even taken place in India. This attack required no technical skill whatsoever; it simply required a psychosocial understanding of the place and time to post to achieve the desired effect.

These last two actions are examples of cognitive hacking. Key to the successes of these cognitive hacks were the *unprecedented speed and extent* of disinformation distribution. Another core element of the success of these two efforts was their authors' correct assessment of their intended audiences' *cognitive vulnerability*—a premise that the audience is already predisposed to accept because it appeals to existing fears or anxieties. [8]

Another particularly instructive incident took place during Operation Valhalla in Iraq in March 2006. A battalion of United States Special Forces Soldiers engaged a Jaish al-Mahdi death squad, killing 16 or 17, capturing 17, destroying a weapons cache, and rescuing a badly beaten hostage. In the time it took for the soldiers to get back to their base—less than one hour—Jaish al-Mahdi soldiers had returned to the scene and rearranged the bodies of their fallen comrades to make it look as if they had been murdered while in the middle of prayer. They then put out pictures and press releases in Arabic and English showing the alleged atrocity.

The U.S. unit had filmed its entire action and could prove this is not what happened, and yet it took almost three days before the U.S. military attempted to tell its side of the story in the media. The Army was forced to launch an investigation that lasted 30 days, during which time the battalion was out of commission. [9]

The Jaish al-Mahdi operation is an excellent example of how social media and the Internet can inflict a defeat without using physical force. This incident was one of the first clear demonstrations of how adversaries can now openly monitor American audience reactions to their messaging, in real time, from thousands of miles away and fine tune their actions accordingly. Social media and the Internet provide our adversaries with unlimited global access to their intended audience, while the U.S. Government is paralyzed by legal and policy issues.

THE RUSSIAN THREAT

In February 2017, Russian Defense Minister Sergey Shoigu openly acknowledged the formation of an Information Army within the Russian military: "Information operations forces have been established that are expected to be a far more effective tool than all we used before for counter-propaganda purposes." [10] The current chief of the Russian General Staff, General Valery Gerasimov, observed that war is now conducted by a roughly 4:1 ratio of nonmilitary and military measures. [11] In the Russian view, these nonmilitary measures of warfare include economic sanctions, disruption of diplomatic ties, and political and diplomatic pressure. The Russians see information operations (IO) as a critical part of nonmilitary measures. They have adapted from well-established Soviet techniques of subversion and destabilization for the age of the Internet and social media.

Russia has a very different view of IO than the United States (or the West in general). For example, a glossary [12] of key information security terms produced by the Russian Military Academy of the General Staff contrasts the fundamental Russian and Western concepts of IO by explaining that for the Russians IO are a continuous activity, regardless of the state of relations with any government, while the West-

---

[8] Waltzman, 2015a.

[9] Rand Waltzman, "The U.S. Is Losing the Social Media War," Time, October 12, 2015b. For a detailed account, see Cori E. Dauber, "The TRUTH Is Out There: Responding to Insurgent Disinformation and Deception Operations, Military Review, January–February 2009.

[10] Ed Adamcyzk, "Russia Has a Cyber Army, Defense Ministry Acknowledges," UPI, February 23, 2017.

[11] Valery Gersimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations," Military Review, January–February 2016.

[12] Voyennaya Akademiya General'nogo Shtaba, *Словарь терминов и определений в о́бласти информационной о́безопасности (Dictionary of Terms and Definitions in the Field of Information Security),* 2nd ed., Moscow Voyeninform, 2008.

erners see IO as limited, tactical activity only appropriate during hostilities.[13] In other words, Russia considers itself in a perpetual state of information warfare, while the West does not.

State-sponsored propaganda and disinformation have been in existence for as long as there have been states. The major difference in the 21st century is the ease, efficiency, and low cost of such efforts. Because audiences worldwide rely on the Internet and social media as primary sources of news and information, they have emerged as an ideal vector of information attack. Most important from the United States perspective, Russian IO techniques, tactics and procedures are developing constantly and rapidly, as continually measuring effectiveness and rapidly evolving techniques are very cheap compared to the costs of any kinetic weapon system—and they could potentially be a lot more effective.

At this point, Russian IO operators use relatively unsophisticated techniques systematically and on a large scale. This relative lack of sophistication leaves them open to detection. For example, existing technology can identify paid troll operations, bots, etc. Another key element of Russian IO strategy is to target audiences with multiple, conflicting narratives to sow seeds of distrust of and doubt about the European Union (EU) as well as national governments. These can also be detected. The current apparent lack of technical sophistication of Russian IO techniques could derive from the fact that, so far, Russian IO has met with minimal resistance. However, if and when target forces start to counter these efforts and/or expose them on a large scale, the Russians are likely to accelerate the improvement of their techniques, leading to a cycle of counter-responses. In other words, an information warfare arms race is likely to ensue.

A STRATEGY TO COUNTER THE RUSSIAN THREAT

Because the culture and history of each country is unique and because the success of any IO defense strategy must be tailored to local institutions and populations, the most effective strategies are likely to be those that are developed and managed on a country-by-country basis. An information defense strategy framework for countering Russian IO offensives should be "whole-of-nation" in character. A whole-of-nation approach is a coordinated effort between national government organizations, military, intelligence community, industry, media, research organizations, academia and citizen organized groups. A discreet US Special Operations Force could provide individual country support as well as cross country coordination.

Just as in the physical world, good maps are critical to any IO strategy. In the case of IO, maps show information flows. Information maps must show connectivity in the information environment and help navigate that environment. They exist as computer software and databases. Information cartography for IO is the art of creating, maintaining, and using such maps. An important feature of information maps is that they are constantly changing to reflect the dynamic nature of the information environment. Because they are artificially intelligent computer programs, they can answer questions; provide situation awareness dynamically; and help to plan, monitor, and appropriately modify operations. Information maps are technically possible today and already exist in forms that can be adapted to support the design and execution IO strategy.

As an example, most of the North Atlantic Treaty Organization (NATO) states, as well as several non-NATO partners, are already subject to concentrated Russian IO and they illustrate ongoing Russian IO techniques. Using information cartography, it is possible to map key Russian sources as part of Russian IO operations against a target state. These sources might include:

- Russian and target country think tanks
- foundations (e.g., Russkiy Mir)
- authorities (e.g., Rossotrudnichestvo)
- television stations (e.g. RT)
- pseudo-news agencies and multimedia services (e.g., Sputnik)
- cross-border social and religious groups
- social media and Internet trolls to challenge democratic values, divide Europe, gather domestic support, and create the perception of failed states in the EU's eastern neighborhood
- Russian regime—controlled companies and organizations
- Russian regime—funded political parties and other organizations in target country in particular and within the EU in general intended to undermine political cohesion

[13] Office of the Under Secretary of Defense for Acquisition and Technology, "Report of the Defense Science Board Task Force on Information Warfare," Washington, D.C., November 1996.

- Russian propaganda directly targeting journalists, politicians, and individuals in target countries in particular and the EU in general.

Similarly, the mapping of target state receivers as part of Russian IO against the target state might include:

- national government organizations
- military
- intelligence community
- industry
- media
- independent think tanks
- academia
- citizen-organized groups.

An effective information defensive strategy would be based on coordinated countering of information flows revealed by information maps. An effective strategy would include methods for establishing trust between elements of the defense force and the public. The strategy also will include mechanisms to detect the continuously evolving nature of the Russian IO threat and rapidly adapt in a coordinated fashion across all defense elements.

Christopher Paul and Miriam Matthews of the RAND Corporation observe: "Experimental research in psychology suggests that the features of the contemporary Russian propaganda model have the potential to be highly effective." [14] They present a careful and concise analysis of relevant psychological research results that should inform any information defensive strategy. For example, they describe how propaganda can be used to distort perceptions of reality:

- People are poor judges of true versus false information—and they do not necessarily remember that particular information was false.
- Information overload leads people to take shortcuts in determining the trustworthiness of messages.
- Familiar themes or messages can be appealing even if they are false.
- Statements are more likely to be accepted if backed by evidence, even if that evidence is false.
- Peripheral cues—such as an appearance of objectivity—can increase the credibility of propaganda. [15]

Here is what a typical offensive strategy against a target population might look like. It consists of several steps:

1. Take the population and break it down into communities, based on any number of criteria (e.g. hobbies, interests, politics, needs, concerns, etc.).
2. Determine who in each community is most susceptible to given types of messages.
3. Determine the social dynamics of communication and flow of ideas within each community.
4. Determine what narratives of different types dominate the conversation in each community.
5. Use all of the above to design and push a narrative likely to succeed in displacing a narrative unfavorable to you with one that is more favorable.
6. Use continual monitoring and interaction to determine the success of your effort and adjust in real time.

Technologies currently exist that make it possible to perform each of these steps continuously and at a large scale. However, while current technologies support manual application of the type of psychological research results presented by Paul and Matthews, they do not fully automate it. That would be the next stage in technology development.

These same technologies can be used for defensive purposes. For example, you could use the techniques for breaking down communities described above to detect adversary efforts to push a narrative and examine that narrative's content. The technology can help researchers focus while searching through massive amounts of social media data.

---

[14] Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model,* Santa Monica, Calif: RAND Corporation, PE–198–OSD, 2016.

[15] Ibid.

WAY AHEAD

"The massive explosion of behavioral data made available by the advent of social media has empowered researchers to make significant advances in our understanding of the dynamics of large groups online. However, as this field of research expands, opportunities multiply to use this understanding to forge powerful new techniques to shape the behavior and beliefs of people globally. These techniques can be tested and refined through the data-rich online spaces of platforms like Twitter, Facebook and, looking to the social multimedia future, Snapchat.

Cognitive security (COGSEC) is a new field that focuses on this evolving frontier, suggesting that in the future, researchers, governments, social platforms, and private actors will be engaged in a continual arms race to influence—and protect from influence—large groups of users online. Although COGSEC emerges from social engineering and discussions of social deception in the computer security space, it differs in a number of important respects. First, whereas the focus in computer security is on the influence of a few individuals, COGSEC focuses on the exploitation of cognitive biases in large public groups. Second, while computer security focuses on deception as a means of compromising computer systems, COGSEC focuses on social influence as an end unto itself. Finally, COGSEC emphasizes formality and quantitative measurement, as distinct from the more qualitative discussions of social engineering in computer security.

What is needed is a Center for Cognitive Security to create and apply the tools needed to discover and maintain fundamental models of our ever-changing information environment and to defend us in that environment both as individuals and collectively. The center will bring together experts working in areas such as cognitive science, computer science, engineering, social science, security, marketing, political campaigning, public policy, and psychology to develop a theoretical as well as an applied engineering methodology for managing the full spectrum of information environment security issues." [16]

The center should be nonprofit and housed in a nonprofit, nongovernmental organization that has international credibility and close ties with government, industry, academia, think tanks, and public interest groups internationally. It should have the following ongoing functions:

1. Bring together experts in a broad range of fields to develop Cognitive Security policies, strategies and implementation approaches.
2. Create clear and practical technology goals in support of the policies and strategies developed.
    i. Identify and evaluate appropriate commercial technologies.
    ii. Identify and evaluate relevant research results and develop and execute strategies for transitioning them into practice.
3. Work with end users from all communities to develop techniques, tactics and procedures for applying technologies identified and developed to policies and strategies.
4. Create a research agenda for policy and strategy formulation, implementation, and supporting technologies.
5. Develop education and training materials and conduct workshops and conferences.
6. Maintain a response team that will coordinate with all communities to identify influence campaigns and distribute alerts and warnings.

This center should be wholly financed for its first five years by the U.S. Government until it can establish additional sources of funding from industry and other private support. The center should also have the authority and funding for grants and contracts, since, apart from a group of core personnel employed by the center, many of the participants will be experts based at their home institution. Although the Center as described would be a non-profit non-governmental organization, this funding model runs the risk of creating the appearance that the U.S. Government has undue influence over its activity. This could raise concerns about the credibility of the Center and the motives of the US Government. An alternative would be to seek a combination of private foundation funding and support from international non-partisan non-governmental organizations (e.g. the United Nations).

[16] Rand Waltzman, "Proposal for a Center for Cognitive Security," *Information Professional Association,* September 2015.

CONCLUSION

We have entered the age of mass customization of messaging, narrative, and persuasion. We need a strategy to counter Russian, as well as others, information operations and prepare the United States organizationally for long-term IO competition with a constantly changing set of adversaries large and small. It is said that where there is a will, there is a way. At this point, ways are available. The question is, do we have the will to use them?

Senator ROUNDS. Thank you, sir.

Mr. Watts, you may begin.

STATEMENT OF CLINT WATTS, ROBERT A. FOX FELLOW, FOREIGN POLICY RESEARCH INSTITUTE

Mr. WATTS. Mr. Chairman, members of the subcommittee, thank you for having me here today. My remarks will include some of what I talked about in my last session at the Senate Select Committee for Intelligence, but also my experience since 2005 working on cyber-enabled influence operations for the U.S. Government in a variety of different capacities.

Russia does five things that sets it apart from others in terms of influence.

One, they create content across deliberate themes, political, social, and financial messages. But they hyper-empower those with hacked materials that act as nuclear fuel for information atomic bombs. These nuclear-fueled bombs are what also power political groups and other profiteers in the social media space that further amplify their messages.

Second, they push in unison from what appear to be many locations at the same time, using both covert and overt accounts and social media platforms.

Third, they share their content through gray outlets and covert personas in a one-to-one and a one-to-many way, such that it looks like a conversation is much larger than it actually is.

Fourth, they discuss themes over enduring period, driving the preferred message deep into the target audience. This collaborative discussion amongst unwitting Americans makes the seemingly improbable, false information seem true.

Finally, they challenge their adversaries online for unnaturally long periods and at peculiar intervals, and push their political opponents down, whether they be politicians, media personalities, or just people that do not like Russian positions.

If there is one thing that I could emphasize today it is that cyber influence is a human challenge, not a technical one. American obsession with social media has overlooked several types of real-world actors that help enable their operations online: Useful idiots such as unwitting Americans that do not realize that they are using Russian information for their political or partisan or even social issue purposes. Fellow travelers, these are personas that have been propped up and promoted across Europe and the United States for their alternative-right positions that are both anti-EU [European Union] and anti-NATO [North Atlantic Treaty Organization]. The last part is agent provocateurs, which are actual people that create incidents such that they can drive traffic online.

If we look back to our experience with ISIS [Islamic State of Iraq and Syria], part of the reason ISIS's social media campaigns did so

well is because they were taking ground and establishing a caliphate. The same happens in the Russian context.

Each of these actors assist Russia's online efforts and have to be dealt with along with the cyber components of it.

When it comes to Americans countering cyber-influence operations, when all is said and done, far more is said than none. We talk about it a lot, but we do fewer iterations than our Russian adversaries. When the U.S. has done something, it has not been effective. At worst, it has been counterproductive. That is due to the way we structure it.

Despite spending hundreds of millions of dollars since 9/11 on United States influence and information operations, we have seen the expansion of al Qaeda and the Islamic State.

We have excessively focused on bureaucracy and digital tech tools. But at the same time, these social media monitoring tools have failed to counter al Qaeda. They did not detect the rise of ISIS, nor did they detect the interference of Russia in our election last year.

America will only succeed in countering cyber influence by turning its current approaches upside down, focusing on the human aspect and using the methodology prioritizing tasks, talent, teamwork, and then technology, in that order.

The first task we have to do is clearly map out the Russian scope of their influence effort, both on the ground and online, so we understand where those two come together.

Second, American politicians, political organizations, and government officials must reaffirm their commitment to fact over fiction by regaining the trust of their constituents through accurate communications.

Third, we must clearly articulate our policy with regards to the European Union, NATO, and immigration, which at present mirrors rather than counters the Kremlin's position.

With regard to talent, U.S. attempts to recruit personnel excessively focus on security clearances and rudimentary training, thus screening out many top picks. A majority of top talent needed for cyber influence that reside in the private sector have no need for a security clearance, have likely used a controlled substance during their lifetime, and can probably work from home easier than they can from a government building. We need to enable that talent rather than screen it out.

In terms of teamwork, U.S. Government influence efforts have fallen into the repeated trap of whole-of-government approaches. Moving forward, we need a task force specifically designated to deal with cyber influence and with the resources and personnel staffed to do it.

Tech tool purchases have excessively focused on social media analytical packages, which I believe are the digital snake oil of the modern era. What we need instead are tools that help us empower our analysts, that are built by our analysts that our coders and programmers that are working with our analysts.

Based on my experience, this is the most successful solution. We build actual custom applications that help us detect the threats that we are wanting to do. We have seen this in the hacking space. The NSA [National Security Agency] and other agencies have done

it. We do not need big, enterprise-wide solutions. We need to rent tools. We do not need to buy them.

With regards to the private sector in the roughly 1 month since I last testified, they have made great strides in restoring the integrity of information by reaffirming the purity of their systems. Facebook, Google, even Wikipedia now have all launched efforts that I applaud and think will make a big difference.

Twitter is the remaining one that I am waiting to hear from, and Twitter is the key cog that is left. Twitter's actions, if they take them on parallel with Facebook and Google and the others, can help shape the Russian influence of the French and the German elections going into summer.

In conclusion, my colleagues and I identified, tracked, and traced, the rise of Russian influence with home computers and a credit card. We can do this if we focus on the humans first, make them the priority, figure out the strategy we want to implement, and back them with the best technology, all of which America has at its doorstep.

Thank you very much.

[The prepared statement of Mr. Watts follows:]

PREPARED STATEMENT BY CLINT WATTS

Mr. Chairman, Members of the Committee. Thank you for inviting me today and for furthering the discussion of cyber-enabled influence. My remarks today will further expand on my previous testimony to the Senate Select Committee on Intelligence on March 30, 2017 where I detailed the research Andrew Weisburd, J.M. Berger and I published regarding Russian attempts to harm our democracy via social media influence.[1] I'll add further to this discussion and will also provide my perspective having worked on cyber-enabled influence operations and supporting programs for the United States Government dating back to 2005. Having served in these Western counterterrorism programs, I believe there are many lessons we should learn from and not repeat in future efforts to fight and win America's information wars.

1) How does Russian nation state influence via social media differ from other influence efforts on social media?

As I discussed on March 30, 2017,[2] Russia, over the past three years, has conducted the most successful influence campaign in history using the Internet and more importantly social media to access and manipulate foreign audiences. Russia and other nation states are not the only influencers in social media. Profiteers pushing false or salacious stories for ad revenue, political campaigns running advertisements and satirists looking for laughs also seek to influence audiences during elections, but their online behavior manifests differently from that of Russia. Russia's hacking may be covert, but their employment of compromat ultimately reveals their overt influence campaigns. Furthermore, Russian influence performs a full range of actions to achieve their objectives that distinguish them from other influence efforts.[3]

- *Create, Push, Share, Discuss, Challenge (CPSDC)—Effective State Sponsors Do All Of These In The Influence Space, Others Do Only Some*
  - *Create*—Russia uses their state sponsored media outlets and associated conspiratorial websites to *create* propaganda across political, social, financial and calamitous message themes. This content, much of which is fake news or ma-

[1] Andrew Weisburd, Clint Watts and JM Berger (6 November 2016) *Trolling For Trump: How Russia Is Trying To Destroy Our Democracy.* War On The Rocks. Available at: *https://warontherocks.com/2016/11/trolling-or-trump-how-russia-is-trying-to-destroy-our-democracy/*

[2] Clint Watts (30 March 2017) Testimony to U.S. Senate Select Committee on Intelligence. *"Russia and 2016 Elections."* Available at: *https://www.c-span.org/video/?426227-1/senate-intelligence-panel-warned-russians-play-sides*.

[3] See Clint Watts and Andrew Weisburd (13 December 2016) *How Russia Wins An Election.* Politico. Available at: *http://www.politico.com/magazine/story/2016/12/how-russia-wins-an-election-214524.*

nipulated truths, provides information missiles tailored for specific portions of an electorate they seek to influence. More importantly, Russia's hacking and theft of secrets provides the nuclear fuel for information atomic bombs delivered by their state sponsored media outlets and covert personas. This information fuels not only their state sponsored outlets but arms the click-bait content development of profiteers and political parties who further amplify Russia's narratives amongst Western voters.

- *Push*—Unlike other fake news dissemination, Russia synchronizes the *push* of their propaganda across multiple outlets and personas. Using sockpuppets and automated bots appearing to be stationed around the world, Russia simultaneously amplifies narratives in such a way to grab mainstream media attention. Many other bots push false and misleading stories for profit or politics but their patterns lack the synchronization and repeated delivery of pro-Russian content and usually follow rather than lead in the dissemination of Russian conspiracies.
- *Share*—Like-minded supporters, aggregators (gray accounts) and covert personas (black accounts) *share* coordinated pushes of Russian propaganda with key nodes on a one-to-one or one-to-many basis. This coordinated sharing seeks to further amplify and cement influential content and their themes amongst a targeted set of voters. Their sharing often involves content appealing to either the left or right side of the political spectrum as well as any anti-government or social issue. This widespread targeting often varies from profiteers and political propagandists that seek a high rate of consumption with a more narrow target audience.
- *Discuss*—Russian overt supporters and covert accounts, unlike other digital influence efforts, *discuss* Russian themes over an enduring period driving the preferred message deep into their target audience. This collaborative discussion amongst unwitting Americans makes seemingly improbable information more believable. Comparatively, bots and campaigns from profiteers, satirists and political propagandists more frequently appear as "fire-and-forget" messaging operations.
- *Challenge*—Heated social media debates during election season have been and will remain commonplace. But Russian influence operations directly *challenge* their adversaries for unnaturally long periods and at peculiar intervals. Russian covert personas heckle and push chosen themes against political opponents, media personalities and subject matter experts to erode target audience support Russian adversaries and their political positions. These challenges sometimes provide the Kremlin the added benefit of diminishing Russian opponent social media use. Other social media influence efforts will not go to such lengths as this well resourced, fully committed Advanced Persistent Threat (APT).

- *Full Spectrum Influence Operations: Synchronization of White, Gray and Black Efforts*—Russian cyber enabled influence operations demonstrate never before seen synchronization of Active Measures. Content created by white outlets (RT and Sputnik News) promoting the release of compromising material will magically generate manipulated truths and falsehoods from conspiratorial websites promoting Russian foreign policy positions, Kremlin preferred candidates or attacking Russian opponents. Hackers, hecklers and honeypots rapidly extend information campaigns amongst foreign audiences. As a comparison, the full spectrum synchronization, scale, repetition and speed of Russia's cyber-enabled information operations far outperform the Islamic State's recently successful terrorism propaganda campaigns or any other electoral campaign seen to date.
- *Cyber-enabled Influence Thrives When Paired with Physical Actors and Their Actions*—American obsession with social media has overlooked the real world actors assisting Russian influence operations in cyber space, specifically "Useful Idiots", "Fellow Travellers" and "Agent Provocateurs".
  - *"Useful Idiots"*—Meddling in the United States and now European elections has been accentuated by Russian cultivation and exploitation of *"Useful Idiots"*—a Soviet era term referring to unwitting American politicians, political groups and government representatives who further amplify Russian influence amongst Western populaces by utilizing Russian compromat and resulting themes.
  - *"Fellow Travellers"*—In some cases, Russia has curried the favor of *"Fellow Travellers"*—a Soviet term referring to individuals ideologically sympathetic to Russia's anti-EU, anti-NATO and anti-immigration ideology. A cast of alternative right characters across Europe and America now openly push Rus-

sia's agenda both on-the-ground and online accelerating the spread of Russia's cyber-enabled influence operations.

- *"Agent Provocateurs"*—Ever more dangerous may be Russia's renewed placement and use of "Agent Provocateurs"—Russian agents or manipulated political supporters who commit or entice others to commit illegal, surreptitious acts to discredit opponent political groups and power falsehoods in cyber space. Shots fired in a Washington, DC pizza parlor by an American who fell victim to a fake news campaign called #PizzaGate demonstrate the potential for cyber-enabled influence to result in real world consequences.[4] While this campaign cannot be directly linked to Russia, the Kremlin currently has the capability to foment, amplify, and through covert social media accounts, encourage Americans to undertake actions either knowingly or unknowingly as Agent Provocatuers.

- Each of these actors assists Russia's online efforts to divide Western electorates across political, social and ethnic lines while maintaining a degree of "plausible deniability" with regards to Kremlin interventions. In general, Russian influence operations targeting closer to Moscow and further from Washington, DC will utilize greater quantities and more advanced levels of human operatives to power cyber-influence operations. Russia's Crimean campaign and their links to a coup in Montenegro demonstrate the blend of real world and cyber influence they can utilize to win over target audiences.[5][6] The physical station or promotion of gray media outlets and overt Russian supporters in Eastern Europe were essential to their influence of the United States Presidential election and sustaining "plausible deniability". It's important to note that America is not immune to infiltration either, physically or virtually. In addition to the Cold War history of Soviet agents recruiting Americans for Active Measures purposes, the recently released dossier gathered by ex MI6 agent Chris Steele alleges on page 8 that Russia used, "Russian migr & associated offensive cyber operatives in United States" during their recent campaign to influence the United States election. While still unverified, if true, employment of such agents of influence in the United States would provide further plausible deniability and provocation capability for Russian cyber-enabled influence operations.[7]

2) How can the U.S. Government counter cyber-enabled influence operations?

When it comes to America countering cyber-enabled influence operations, when all is said and done, far more is said than done. When the U.S. has done something to date, at best, it has been ineffective, and at worst, it has been counterproductive. Despite spending hundreds of millions of dollars since 9/11, United States influence operations have made little or no progress in countering al Qaeda, its spawn the Islamic State or any connected jihadist threat group radicalizing and recruiting via social media.

Policymakers and strategists should take note of this failure before rapidly plunging into an information battle with state sponsored cyber-enabled influence operations coupled with widespread hacking operations—a far more complex threat than any previous terrorist actor we've encountered. Thus far, United States cyber influence has been excessively focused on bureaucracy and expensive technology tools—social media monitoring systems that have failed to detect the Arab Spring, the rise of ISIS, the Islamic State's taking of Mosul and most recently Russia's influence of the United States election. America will only succeed in countering Russian influence by turning its current approaches upside down, clearly determining what it seeks to achieve with its counter influence strategy and then harnessing top talent empowered rather than shackled by technology.

- *Task*—Witnessing the frightening possibility of Russian interference in the recent United States Presidential election, American policy makers have immediately called to counter Russian cyber influence. But the United States should take pause in rushing into such efforts. The United States and Europe

---

[4] Amy Davidson (5 December 2016) "The Age of Donald Trump and Pizzagate." The New Yorker. Available at: *http://www.newyorker.com/news/amy-davidson/the-age-of-donald-trump-and-pizzagate*

[5] Mike Mariani (28 March 2017) "Is Trump's Chaos Tornado A Move From The Kremlin's Playbook?" Vanity Fair. Available at: *http://www.vanityfair.com/news/2017/03/is-trumps-chaos-a-move-from-the-kremlins-playbook*

[6] Bellingcat (25 April 2017) "Montenegro Coup Suspect Linked to Russian-backed "Ultranationalist" Organization." Available at: *https://www.bellingcat.com/news/uk-and-europe/2017/04/25/montenegro-coup-suspect-linked-russian-backed-ultranationalist-organisation/*

[7] See Buzzfeed release of Chris Steele unverified dossier at the following link: *https://www.documentcloud.org/documents/3259984-Trump-Intelligence-Allegations.html*

lack a firm understanding of what is currently taking place. The United States should begin by clearly mapping out the purpose and scope of Russian cyber influence methods. Second, American politicians, political organizations and government officials must reaffirm their commitment to fact over fiction by regaining the trust of their constituents through accurate communications. They must also end their use of Russian compromat stolen from American citizens' private communications as ammunition in political contests. Third, the United States must clearly articulate its policy with regards to the European Union, NATO and immigration, which, at present, mirrors rather than counters that of the Kremlin. Only after these three actions have been completed, can the United States Government undertake efforts to meet the challenge of Russian information warfare through its agencies as I detailed during my previous testimony.

- *Talent*—Russia's dominance in cyber-enabled influence operations arises not from their employment of sophisticated technology, but through the employment of top talent. Actual humans, not artificial intelligence, achieved Russia's recent success in information warfare. Rather than developing cyber operatives internally, Russia leverages an asymmetric advantage by which they coopt, compromise or coerce components of Russia's cyber criminal underground. Russia deliberately brings select individuals into their ranks, such as those GRU leaders and proxies designated in the 29 December 2016 United States sanctions. Others in Russia with access to sophisticated malware, hacking techniques or botnets are compelled to act on behalf of the Kremlin.

  The U.S. has top talent for cyber influence but will be unlikely and unable to leverage it against its adversaries. The U.S. focuses excessively on technologists failing to blend them with needed information campaign tacticians and threat analysts. Even further, U.S. agency attempts to recruit cyber and influence operation personnel excessively focus on security clearances and rudimentary training thus screening out many top picks. Those few that can pass these screening criteria are placed in restrictive information environments deep inside government buildings and limited to a narrow set of tools. The end result is a lesser-qualified cyber-influence cadre with limited capability relying on outside contractors to read, collate and parse open source information from the Internet on their behalf. The majority of the top talent needed for cyber-enabled influence resides in the private sector, has no need for a security clearance, has likely used a controlled substance during their lifetime and can probably work from home easier and more successfully than they could from a government building.
- *Teamwork*—Russia's cyber-enabled influence operations excel because they seamlessly integrate cyber operations, influence efforts, intelligence operatives and diplomats into a cohesive strategy. Russia doesn't obsess over their bureaucracy and employs competing and even overlapping efforts at times to win their objectives.

  Meanwhile, U.S. Government counter influence efforts have fallen into the repeated trap of pursuing bureaucratic whole-of-government approaches. Whether it is terror groups or nation states, these approaches assign tangential tasks to competing bureaucratic entities focused on their primary mission more than countering cyber influence. Whole-of-government approaches to countering cyber influence assign no responsible entity with the authority and needed resources to tackle our country's cyber adversaries. Moving forward, a Task Force led by a single agency must be created to counter the rise of Russian cyber-enabled operations. Threat based analysis rather than data analytics will be essential in meeting the challenge of Russian cyber influence operations. This common operational picture must be shared with a unified task force, not shared piecemeal across a sprawling interagency.
- *Technology*—Over more than a decade, I've repeatedly observed the U.S. buying technology tools in the cyber-influence space for problems they don't fully understand. These tech tool purchases have excessively focused on social media analytical packages producing an incomprehensible array of charts depicting connected dots with different colored lines. Many of these technology products represent nothing more than modern snake oil for the digital age. They may work well for Internet marketing but routinely muddy the waters for understanding cyber influence and the bad actors hiding amongst social media storm.

Detecting cyber influence operations requires the identification of specific needles, amongst stacks of needles hidden in massive haystacks. These needles are cyber hackers and influencers seeking to hide their hand in the social media universe. Based on my experience, the most successful technology for identifying cyber and influence actors comes from talented analysts that first comprehensively identify threat actor intentions and techniques and then build automated applications specifically tailored to detect these actors. The U.S. Government should not buy these technical tools nor seek to build expensive, enterprise-wide solutions for cyber-influence analytics that rapidly become outdated and obsolete. Instead, top talent should be allowed to nimbly purchase or rent the latest and best tools on the market for whatever current or emerging social media platforms or hacker malware kits arise.

3) What can the public and private sector do to counter influence operations?

I've already outlined my recommendations for United States Government actions to thwart Russia's Active Measures online in my previous testimony on 30 March 2017.[8] Social media companies and mainstream media outlets must restore the integrity of information by reaffirming the purity of their systems. In the roughly one month since I last testified however, the private sector has made significant advances in this regard. Facebook has led the way, continuing their efforts to reduce fake news distribution and removing up to 30,000 false accounts from its system just this past week. Google has added a fact checking function to their search engine for news stories and further refined its search algorithm to sideline false and misleading information. Wikipedia launched a crowd-funded effort to fight fake news this week. The key remaining private sector participant is Twitter, as their platform remains an essential networking and dissemination vector for cyber-enabled influence operations. Their participation in fighting fake news and nefarious cyber influence will be essential. I hope they will follow the efforts of other social media platforms as their identification and elimination of fake news spreading bots and false accounts may provide a critical block to Russian manipulation and influence of the upcoming French and German elections.

In conclusion, my colleagues and I identified, tracked and traced the rise of Russian influence operations on social media with home computers and some credit cards. While cyber-influence operations may appear highly technical in execution, they are very human in design and implementation. Technology and money will not be the challenge for America in countering Russia's online Active Measures; it will be humans and the bureaucracies America has created that prevent our country from employing its most talented cyber savants against the greatest enemies to our democracy.

[8] Clint Watts. "Russia's Info War on the U.S. Started in 2014" The Daily Beast. Available at: *http://www.thedailybeast.com/articles/2017/03/30/russia-s-info-war-on-the-u-s-started-in-2014.html*

Russia's "Active Measures" - Blending Overt To The Covert On Social Media

Source: A. Weisburd (CCHS) C. Watts (FPRI & CCHS) J. Berger (ICCT)

Senator ROUNDS. Thank you, sir.

I will begin the questions, and we will move around through here, 5 minutes each on questions.

I do have a specific question for Mr. Inglis.

You were a member of the Defense Science Board Task Force on Cyber Deterrence, and we have had an opportunity to review both the classified and the unclassified report.

As I mentioned in my opening remarks, the Task Force determined that the deterrence of Russian and China in cyberspace was urgently needed because, for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructure.

I am just curious, in your opinion, as a member of the board, can cyber deterrence apply to cyber-enabled information operation campaigns like that which we experienced last year? If it can, what unique challenges does this gray zone warfare, like information operations, pose for deterrence frameworks?

Mr. INGLIS. Thank you for the question. I begin by saying, I was privileged to serve on that panel, and the comments I am about to make are derived from my experience on that panel, but not on behalf of that panel.

I would say that I do think that it can apply. It has some natural limits. There are, of course, deterrents of two kinds in classic deterrence theory. The first is deterrence by denial, that you simply deny your adversary an opportunity to careen into your well-laid plans or your forward momentum through a variety of methods. The second is deterrence by cost imposition. I think both of those could apply here, but I think the cost imposition probably will be the weaker of the two.

But it is interesting to take a look. There was a recent op-ed—I believe it was in Politico.com—about why Finland is not concerned about Russian interference in their election. It is not because Russia is not interfering in their election. It is because of two things.

One, Finland actually well understands the nature of Russia and what they do, and the means and methods by which they do it. It is easier for them to identify, from citizens up to leaders, what the Russians are up to and what they are up to.

But more importantly, Finland has defined from the top down their own message, their own strategy, their own strategic gains. Then they take great pains to communicate that latterly, horizontally, and vertically, such that it is very hard to careen into that message. I think that is deterrence by denial in the information war.

Therefore, I do think that that theory can help us in this space.

Senator ROUNDS. Thank you.

For all of you, I would just like to work my way down the line here. I will ask each of you to respond.

Much of the Russian activity in the run-up to the United States presidential election appears to have been enabled by loose or outdated cybersecurity controls. What can the government do to better protect its networks and the information residing therein?

Some of the data breaches occurred, as we all know, on non-governmental systems that are not considered part of DHS's [Department of Homeland Security] 16 designated critical infrastructure sectors. How can the government encourage these private sector network owners and operators to better protect their networks?

We had both, those that looked both in government and out of the government.

I will begin with you, sir, if you would like, and we will work our way back down the line.

Mr. WATTS. I think the big challenge is that most of this happens outside government networks, so even if you are a government official or a former government official, they are going to hit you when you are not in your workspace.

That is partly because attacking the government network can be seen as an act of war, whereas it is more in the gray zone if they hit you on your personal network. That is a deliberate strategy they pursue.

I think the other thing is the controls developed in the private sector are much stronger than we ever see in the government sector. For example, whenever my colleagues and I write about Russia, we get attacked on our Gmail accounts. But Gmail not only notifies us that we are being attacked but says that you are being targeted by a foreign nation, which helps us with our research, ironically. We know that we are on the right track because they tell us that we are on the right track.

But I think those controls, working with private sector and not trying to create them from the inside—we have a tendency in government to say we need to build a thing to do it. It is figuring out how we work with the private sector, whether it is in the financial or even in the social media space—they tend to develop these solutions quicker—and how we migrate those back, number one, into the government, and even to government employees and officials, our people that are being targeted, so they have the best and most sophisticated defenses that are out there.

Senator ROUNDS. Thank you.

Dr. Waltzman?

Dr. WALTZMAN. I think one of the most important things, actually, when it comes to private industry, where I would agree that this is where we need to really focus our efforts, is in getting people to cooperate with each other. This is a really huge problem.

How do you get people to share problems, to say this is what is happening to me now, this is what happened to me yesterday, what is happening to you? Of course, people are reluctant to admit that they have been attacked, that they suffered a big loss. They do not want their shareholders to find out. Something that we could do to try to encourage that kind of cooperation I think would be very important.

Senator ROUNDS. Mr. Lumpkin?

Mr. LUMPKIN. There are technical issues to prevent access by our adversaries to our networks. One of the big challenges we have is the component of training, the training of people who are using these networks to make sure they do not avail themselves to phishing operations and provide access to the networks by our adversaries unwittingly. My experience is the protocols are in place,

but it is usually, when there is access achieved by our adversaries, it is because the human factor was not in compliance for what needed to be done.

I think it is about enforcement of the rules and holding people accountable who do not live up to the expectations of the rules.

Mr. INGLIS. I subscribe to all that has been said so far. I would just simply emphasize again that the activity undertaken by Facebook, Google, and some others to essentially try to create authoritative corroboration of what might otherwise be disparate, diverse news sets is very important in this space. Most of that takes place in the private sector.

The government's role can be to perhaps create a venue for that, some space for that, and to collaborate with other like-minded governments to see if we cannot make that run across international boundaries in ways that might not be natural.

Senator ROUNDS. Thank you.

Senator Nelson?

Senator NELSON. Thank you, Mr. Chairman.

The Russians, be it the Soviet Union or today, have been doing this kind of stuff for a long time. But with the new tools that you all have talked about, we are seeing a different and effective kind, where you can actually have the intent of affecting the outcome of an election upon which a democracy absolutely depends that it is protected, as well as the confidence in that election is protected.

Now, that is going on right now. It is going on in France, and it has been going on and will go on in Germany.

If this is a new normal, what do we do to inoculate the public with call it resilience against this kind of campaign that ultimately ends up being misinformation or call it fake news or whatever you want to call it? What do we do in the future?

Mr. LUMPKIN. As I look at this problem, it is about the credibility of the source. When I look at the information space, and I see the inundation, what I call information toxicity that I feel every day of so much information coming in, it is about finding those sources that have proven to be credible for me.

I think that translates across the spectrum, going back to what Clint Watts was talking about earlier. You have to make sure, as a U.S. Government, our information is accurate and that we are a reliable source of information for consumption of the American people as well as international community as well.

I think that is a good first step in making sure that the American people have a good place to go to get information, which has not always been the case.

Senator NELSON. What is that source?

Mr. LUMPKIN. As the information environment has changed, our organization of how we manage information as the U.S. Government has not changed. Again, this goes back to my opening comments of public diplomacy, public affairs, and information warfare. Each one is governed by different authorities, has different people giving the message.

But those three things in a hyperconnected world are not coordinated. What an embassy may say abroad can be consumed by the U.S. audience at real time. What is said here domestically can have impacts overseas real time. We have to find a way to synchronize

our overall messaging as a U.S. Government, which we have not done to date.

Senator NELSON. All right. But I am thinking something that the government cannot synchronize, and that is the rough and tumble of an election.

Mr. Inglis?

Mr. INGLIS. I was not going to address the rough-and-tumble of an election, but we can come back to that. I was going to support the argument and say that it is very difficult, given what was suggested, and I think that is right, if you go second. You need to go first.

You need to actually establish the momentum, the forward momentum, of a credible idea, a credible source, the corroboration of that source, before you then are chasing the allegations or the vilifying data that might otherwise contest for the time and space.

Senator NELSON. Do we, as a government, need to make sure that everybody in America understands that Russia Today is a fake site?

Mr. INGLIS. I do not think it is necessarily a fake site. It is a source of data. It is not one and the same as information or truth. Therefore, it is a useful influence on how we think about the world. It might, in fact, convey to us Russia's perception, but that is not one and the same as an articulation of our values or an articulation of what is true.

But if we get on message, and it is not necessarily going to be a monolithic message, because we are a set of diverse people—that is a feature here. But if we are on message and we try to actually talk about that in a positive, forward view, and, at the same time, we educate our people, the people who essentially live in that swirl of information, about the nature of information war and what their duties are to try to figure out whether they actually have a grasp on a fact, the sum of those two things I think will make a difference.

Government can lead in that. The private sector already is.

Senator NELSON. Translate what you just said with an example. An obvious fake news story has been put out by Russia Today. Now how is that——

Mr. INGLIS. Let me give you a very personal example.

Senator NELSON. Please.

Mr. INGLIS. I have testified many times before this group and others on the summer of 2013, trying to explain what NSA was really doing with the——

Senator NELSON. What?

Mr. INGLIS. What the National Security Agency was really doing with the telephone metadata or other such programs.

Senator NELSON. Right.

Mr. INGLIS. The challenge there was not that I think we were found in the wrong place. It was that we had not told a story that people could say that there is actually a true story associated with this. We then spent the summer and some time since chasing the allegations, which were not one and the same as revelations.

If we had gone first, if we had essentially said, here is what we do, here is how we do it, and essentially created a backdrop such that when fake news or an alternative version of that, Edward

Snowden's version of that, came into view, people would have said: No, no, I have actually had a chance to think my way through this. I understand what they do. I may not be comfortable with that policy, but I have actually already heard the story from credible, competent sources.

But we went second, and that, therefore, made it all the more difficult for us to put that back in the box.

Senator NELSON. Okay, I agree with that. But you try to explain metadata and people do not understand that.

Mr. INGLIS. I took care not to in the moment that just past because that is less the issue than it is about, is the government actually exercising some national security authorities?

Senator NELSON. Well, what folks needed to understand is that metadata was business records of phone calls.

Mr. INGLIS. Of course, they did. But you start with principles and say, look, the government, in pursuit of national security but not at the detriment, not while holding liberty at risk, exercises certain authorities. We are collecting data.

People pause and say, okay, let me think about that. What kind of data?

You have essentially set the stage by saying what the value proposition is upfront. Then you can have a discussion on the details.

We too often lead with the details, which people are left to imagine what the value proposition that rides on top of that is, and that then leads to discord.

Mr. WATTS. When I testified last time, we had put forth the idea of an information consumer reports in social media, essentially a rating agency that sits apart from the government that rates all media outlets over time and gives them a score.

That score is based on the accuracy of reporting, many variables like you used to remember from the Consumer Reports magazine. It is openly available by that rating agency, and it is put next to every story that pops up on Facebook, Google, Twitter, whatever it might be, such that the consumer, if they want to read about aliens invading the United States, they can, but they know that the accuracy of that is about 10 percent from that outlet. They then have the decision ability to decide what they want to consume.

Google and Facebook have already started to move in this way and have already done fact-checking, Snopes kinds of things that say that this is true or false, and are building that in.

I think they will get to that point where, essentially, you are giving people a nutrition label for information. If they want to eat a 10,000-calorie meal, then they can go ahead and do that. But they know why they are fat, and they know why they are dumb, and they know that the information they are consuming is not good for them.

Senator NELSON. What is your rating of the National Enquirer?

Mr. WATTS. The National Enquirer would be extremely low. I would put RT at 70 percent, just by my examination and some research.

Senator NELSON. Seventy percent accuracy?

Mr. WATTS. Seventy percent true, 20 percent manipulated truth, 10 percent false. That is what I would assess it at over time.

It is actually not that much different than some mainstream outlets that would be rated. That rating system would help mainstream outlets as well. They would have to improve so that their rating gets higher. That check goes across everybody.

If an outlet pops up and 5 days later they are putting out fake news with high traffic, people would know, oh, this is an outlet that just popped up and it is probably propaganda.

The two things the government can do to stop that same sort of rumint, or rumor intelligence, is put up a site at both the State Department and the Department of Homeland Security. Any propaganda that is put out by a foreign nation that directly has a connection to the U.S. Government—for example, the fake Incirlik attack last summer in Turkey that the Russian RT and Sputnik news tried to promote, the State Department immediately comes up and says here is live footage from Incirlik Air Base. There is no siege going on. We have extra security in place because the Chairman of the Joint Chiefs is coming tomorrow.

That is a technique that actually came out of counterterrorism in Iraq from 10 years ago where we had rapid response teams that would go out when there was terrorist propaganda. We would say: Here is live footage of it. It did not happen. Here is what was actually at the scene.

DHS needs to do that as well, because sometimes state actors will try to influence the public to think that crises in the United States are bigger than they are. If there is an airport evacuation, that is ripe material for cyber influence by Russia, to amplify that and create concern and panic in the United States.

We need both a domestic component of it and an international foreign policy component of it.

Those three things combined, I think the private sector will lead in this, and they are already doing a lot for it, will have a huge impact on that false news being spread around the Internet.

Senator ROUNDS. Senator Blumenthal?

Senator BLUMENTHAL. Thanks, Mr. Chairman. Thanks for having this hearing.

Thank you all for being here and for your great work. We are only going to touch the surface of this very complex and profoundly significant topic.

I am just a lawyer. I do not have the technical expertise that you do. Our system of laws typically relies on what judges have called the marketplace of ideas to enable the truth to win. There are all kinds of sayings in the law about how sunlight is the best disinfectant, about how the cure for lack of truth is more truth, which perhaps is an outdated view about what the modern information world looks like.

Mark Twain may have had it right when he said, I am going to butcher this quote, but, falsehood is halfway around the world by the time the truth gets out of bed. Falsehood is so much more easily spread because sometimes it is so much more interesting and has the immediacy of a lie in grabbing people's attention, where the truth is often mundane and boring.

I want to go to a point that you made, Mr. Watts, looking at your testimony. I am going to quote. "Witnessing the frightening possi-

bility of Russian interference in the recent United States presidential election," and you go on.

Is there any doubt in your mind that the Russians did, in fact, interfere? It was more than a frightening possibility. They did interfere. I think the intelligence community is fairly unanimous on that point.

Mr. WATTS. Yes, that is correct. What I was trying to illustrate is that this possibility got us to focus too heavily on the technological aspects and the social media aspects of it.

If you remember in the lead up to the election, we were obsessed about machines being hacked or votes being changed. That was deliberate. That is one of the Russian influence lines, was, "Oh, by the way, even if the election comes out, the election is rigged. There is voter fraud rampant. You cannot trust anything."

That is about active measures. That is about eroding confidence in democracy. Essentially, even when an elected official wins, you do not trust them to be your leader. You think they got there under false pretenses.

Senator BLUMENTHAL. That is what one of the candidates was saying too, correct?

Mr. WATTS. Correct. We have seen that repeatedly, and you are going to see that in other elections around the world.

Senator BLUMENTHAL. Which leads to the suspicion, and there is increasing proof of it, that maybe Trump associates were involved in some way in either supporting or aiding or colluding with these Russian efforts.

I am not asking you to reach a conclusion, but that is under investigation now by the FBI [Federal Bureau of Investigation], correct? All of the three kinds of individuals, the fellow travelers, the friendly idiots, and agent provocateurs, may have been involved, correct, in this Russian effort?

Mr. WATTS. Yes. Cyber influence, we keep separating out the technical and the human. Cyber influence is most effective when you have humans also empowering them, human-empowered action.

You have seen this repeatedly across all elections, which is they either target their propaganda so they can arm certain campaigns against another campaign. That is what hacking is about. "I am going to target some people with hacks, such that I have secrets that I can arm their propaganda as well." That is the amplification of it.

The other part is they are picking candidates and backing them either by supporting them or even on the ground through political parties and potentially funding across Europe.

The last part is, if they do not have the right actions to promote on social media, they will create them. Incirlik is a half-baked attempt. There is a small protest. They turned it into a terrorist attack. If there is not something to drive an election, they might create it. A tactic of classic active measures is, if I need a terrorist attack to foment an audience to swing an election a certain way, maybe the way you saw in Spain in 2004, or more recently even in France, they might create those actions such that they can have that in cyberspace in their influence network to power the candidate they want to move in one direction or the other.

Senator BLUMENTHAL. In terms of recruiting the talent, since the human factor, as you say, is so important—and I am assuming that others on the panel agree that attracting qualified people in this effort is really critically important. We can buy all the machinery will want, but the talent is attracted to other venues and corporations where they often are paid more.

I think this effort is worth a whole study, and a very urgent one, in and of itself. I have heard our military leaders sitting where you are saying we need to recruit these folks, and we are having trouble doing it because there is a limited pool and it pays a lot more to go work for Google or whatever Silicon Valley corporation, startups, and so forth.

Mr. WATTS. I do not know that I always buy into the money aspect of it, to be honest. I work in the private sector as a consultant a lot. The work is really boring compared to being in the government. You might get paid more, but, to be honest with you, you are not going to be too excited at the end of the day.

There are motivated Americans out there that are incentivized by more than just money. Maybe they have gone and made a lot of money and they want to reinvest in their country. I think right now there is an upsurge of people that are not excited about Russia possibly manipulating people's thoughts and minds and views in a way that is anti-American. I think there are a lot of people who would want to join in.

The problem is, when we bring those people into the government space, we take everything that made them great or gave them the space to be great away from them, and then we say we want you to be like a soldier and a private, and you need to do all these other things and take 37,000 hours of mandatory training so that you can operate this computer which does not have the software you have at your house.

That is what even the most inspired Americans out there who are savvy in tech look at—I know I look at it. I say, man, I can do a lot more outside the government than I can do inside.

Until we give them the space to be the tech savants that they are, they are never going to want to come in and stay. They might come in for a while, but ultimately, they will leave because they are motivated but frustrated.

Senator ROUNDS. Dr. Waltzman, you did not get a chance to respond to Senator Blumenthal's question. I think it is a good one. Would you care to respond to that?

Mr. WALTZMAN. Yes. There is one additional thing. Everything Clint said is true, except that there is more, and it is actually even worse.

The problem is that a young person would get to wherever they are going to go in the government, and they are going to be gung-ho and ready to act, and then they are going to find out, well, gee, we have all of these spectacular restrictions and lawyers and all kinds of problems. Never mind about all of the other things you have to do. There are so many restrictions on what you are able to do that they sit there and say, okay, why am I doing this to begin with? If they are not going to actually let me do the job because of all of these problems, why am I here?

That is an even bigger problem. If that can be overcome, the money, I do not think, is the big issue. All these other things, the time to take from people, is not the big issue.

That is the central issue. They come because they are patriotic. They want to do the job. You do not allow them because of these rules.

Senator BLUMENTHAL. My time has expired, and I have more questions that perhaps I can submit to the panel. Unfortunately, I have to go to another commitment. But I just want to thank you all for your service to our Nation, each of you has an extraordinary record of public service, and suggest that perhaps that record of public service reflects motivations and instincts and a worldview that is not shared because you have committed your lives to public service necessarily by the broader American public.

But I hope you are right, that people would be attracted. Also, to just add a caveat, perhaps, to the point that you made so well about the screening. You will remember that, to our sorrow, we encountered situations where the screening seemed to be inadequate to rid ourselves of the Snowdens before they did what they did. That, in turn, precipitated a major sort of effort to clamp down.

There is a balance here, and I recognize that, if you screen out everybody who loves to work in socks at home, or at some point during their education used a controlled substance, you may deprive yourself of the most creative and ingenious of the talent. But it is a dilemma how we screen. I take that point.

Senator ROUNDS. Let me, briefly, the cyber lawyer of the future is going to look different than perhaps what a lawyer looks like today. But I would like, as long as Senator Blumenthal is still here, one item of clarification I would like, in terms of your statement, Mr. Watts, the integrity of the elections was influenced because they suggested it was influenced. I do not believe there was actually any evidence found where they actually did anything.

Do you just want to clarify that a little bit?

Mr. WATTS. Yes. I do not believe that any election systems were hacked into. I do not believe that any votes were changed. Their goal was to create the perception there might have been so that they could further drive wedges inside the U.S. electorate.

I definitely want to clarify that. I saw no evidence of it. It was a theme. It was not an actual truth or an action that occurred.

Senator ROUNDS. Thank you.

You had one quick response to Senator Blumenthal?

Mr. WATTS. Yes. I think one of the things that we have gone to in the post-9/11 world is that everyone has to have a security clearance and access to everything.

Influence is an open business. I can understand it on the technical side, dealing with hacking and cyber lawyers. But there are two components to this.

The other part is just understanding information, social media, and how counter-influence would be done. That does not require a clearance.

It is so much easier for me to track an influence effort for a terrorist group or a nation-state by sitting at my house than it is in the government. I do not need access to classified information to do that part of it.

It helps at the higher levels. Obviously, you need some program managers, your key decision-makers, to be able to see both sides of it. But we do not need to bring everybody into the government and force them to have a security clearance so they can never look at classified information, which happens quite a bit. I think the goal is we bring in the best talent, and we put them in a place where we still protect our secrets.

I do understand your point about Edward Snowden and some of these others. They had clearances. They had access to information they did not need and then stole it. I think, actually, we give them no classified information. I think what we set them on is most of this stuff is happening in the open source.

Even the investigations of cyber are happening in the dark web, but that is accessible outside the government. I do think, with our top cyber people that are doing programming, hacking, those sorts of things at the NSA and other intel agencies, then that obviously makes sense, that they be cleared and heavily scrutinized and monitored.

Senator BLUMENTHAL. I think that is a really important point. It is a little bit like in my world. I used to be a prosecutor.

Our informants do not pass security clearance. Our witnesses often would never even come close to passing a security clearance. But as we used to argue to the jury, not everyone involved in this criminal drug conspiracy is going to be a choir boy. You can use those folks to ferret out information and to track down—I mean, not that they are going to be people we recruit from the other side. But, you are right, they do not necessarily—that is why it is just analogous. It is not an exact comparison.

Mr. WATTS. I can give you an example of who I would hire right now. I would hire the people who were making fake news leading up to the election. If they are good at making fake news for clicks and getting ad revenue, they would be the first people I would hire to come in and tell me what fake news looks like on the Internet. They know how to make it, so they are the best ones at detecting it.

They would be great candidates. You could go to them and say, oh, by the way, you might have been doing some nefarious things that were not quite right, but you could rectify that by coming on board and telling us about others who are doing something similar to you.

Senator BLUMENTHAL. They would probably recognize M.O. [Modus Operandi] of whoever was producing——

Mr. WATTS. For sure.

Senator BLUMENTHAL.—because they have a pretty good guess as to who was producing.

Mr. WATTS. Yes.

Senator ROUNDS. Very good.

Senator BLUMENTHAL. Thank you, Mr. Chairman. I apologize, but this is a fascinating topic.

Senator ROUNDS. It is, and part of a small subcommittee is that, once in a while, you can take a little leeway. Our goal here is to get results.

We are learning, as this is a new subcommittee. As we get into this new stuff, everything that you are providing us is new information to us.

I think the message that most of our members would tell you is that we do not know much about cybersecurity, and what we are trying to do is to learn it and to make good decisions, and that means getting good information.

We most certainly appreciate your participation with this subcommittee today.

Once again, your full statements will be accepted into the record.

Senator Blumenthal, do you have anything else?

We will call this meeting adjourned. Thank you.

[Whereupon, at 3:35 p.m., the subcommittee was adjourned.]