Stenographic Transcript
Before the

Subcommittee on Cybersecurity

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

CYBER-ENABLED INFORMATION OPERATIONS

Thursday, April 27, 2017

Washington, D.C.

ALDERSON COURT REPORTING

1155 CONNECTICUT AVENUE, N.W.

SUITE 200

WASHINGTON, D.C. 20036

(202) 289-2260

www.aldersonreporting.com

CYBER-ENABLED INFORMATION OPERATIONS

Thursday, April 27, 2017

U.S. Senate
Subcommittee on Cybersecurity
Committee on Armed Services
Washington, D.C.

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

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

OPENING STATEMENT OF HON. MIKE ROUNDS, U.S. SENATOR FROM SOUTH DAKOTA

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 a 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 HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

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

And 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. And 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. And 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.

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

So 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.

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

The Chairman: 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. And 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. And 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. And 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.

And then 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:]

Senator Rounds: Thank you, Mr. Inglis.

Mr. Lumpkin, would you care to begin?

STATEMENT OF HON. 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 expanded the GEC's 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 U.S. 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 U.S. 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:]

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. And 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.

So 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. And 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 manipulation. 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.

So 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. And yet, it brought the thing to its knees and destroyed the operation.

So 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. And 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? And third, what kind of organizational structure is needed to manage cognitive security?

And for further details, I refer you to my written testimony.

Thank you.

[The prepared statement of Dr. Waltzman follows:]

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 and anti-NATO. And 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, 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. And at worst, it has been counterproductive. And that is due to the way we structure it.

Despite spending hundreds of millions of dollars since 9/11 on U.S. 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 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:]

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? And 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. So 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.

So, 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 U.S. 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?

And some of the data breaches occurred, as we all know, on nongovernmental systems that are not considered part of DHS's 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. So, 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: So 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. So 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.

So 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.

So 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.

So 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: And 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. So what an Embassy may say abroad can be

consumed by the U.S. audience at real time. And what is said here domestically can have impacts overseas real time. So 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: So 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. So 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: So what is your rating of the National Enquirer?

Mr. Watts: So 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. So 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 U.S.

So 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. And thanks for having this hearing.

And 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. And 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 possibility of Russian interference in the recent U.S. 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. And 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, correct? And 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. And 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.

So that is what even the most inspired Americans out there who are savvy in tech look at -- I know I look at it. And 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. So 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?

So that is an even bigger problem. And 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. And 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. And 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.

So 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.

So 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. So 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. And 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. And 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. 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. And 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.

[The information referred to follows:]

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