Naval Postgraduate School Center for Homeland Defense and Security
HSDL Homeland Security Digital Library
Securing The Homeland Through The Power of Information

April 27, 2017

Cyber-enabled Information Operations

Subcommittee on Cybersecurity, Committee on Armed Services, United States Senate, One Hundred Fifteenth Congress, First Session

---

Hearing Contents:

Witnesses

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

This hearing compilation was prepared by the Homeland Security Digital Library, Naval Postgraduate School, Center for Homeland Defense and Security.

NAVAL POSTGRADUATE SCHOOL CENTER FOR HOMELAND DEFENSE AND SECURITY
HOMELAND SECURITY DIGITAL LIBRARY
SECURING THE HOMELAND THROUGH THE POWER OF INFORMATION

Available Webcast(s)*:

Watch Full Hearing

Compiled From*:

https://www.armed-services.senate.gov/hearings/17-04-27-cyber-enabled-information-operations

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

This hearing compilation was prepared by the Homeland Security Digital Library, Naval Postgraduate School, Center for Homeland Defense and Security.

STATEMENT OF

CHRIS INGLIS

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

27 April 2017

VERSION: 23 April 2017

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.
- So, 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 employed. 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 US 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.

And 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.

STATEMENT OF

HONORABLE MICHAEL D. LUMPKIN

PRINCIPAL

NEPTUNE

BEFORE THE 115TH CONGRESS

SENATE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY

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 US 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 US 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 US 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 US government thinking on shaping and responding in the information environment has remained unchanged, to include how we manage US 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 US government below the President of the United States who is responsible and capable of managing US 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 US 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 US 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 US 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 US 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 US 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 US 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 ast the information environment itself and time ~~lateness for~~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 US 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 FY17 is below $40M. Again, please keep in mind that this is a significant increase from the GEC FY15 budget of $5.6M. 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 US 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.

Testimony

The Weaponization of Information

The Need for Cognitive Security

Rand Waltzman

CT-473
Testimony presented before the Senate Armed Services Committee, Subcommittee on Cybersecurity on April 27, 2017.

RAND CORPORATION

For more information on this publication, visit www.rand.org/pubs/testimonies/CT473.html

Testimonies

RAND testimonies record testimony presented or submitted by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies.

Published by the RAND Corporation, Santa Monica, Calif.
© Copyright 2017 RAND Corporation
RAND® is a registered trademark.

Limited Print and Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited. Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Permission is required from RAND to reproduce, or reuse in another form, any of its research documents for commercial use. For information on reprint and linking permissions, please visit www.rand.org/pubs/permissions.html.

The Weaponization of Information

Testimony of Rand Waltzman[1]
The RAND Corporation[2]

Before the Committee on Armed Services
Subcommittee on Cybersecurity
United States Senate

April 27, 2017

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

---

[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.

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 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

---

[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.

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 U.S. Special Forces Soldiers engaged a Jaish al-Mahdi death squad, killing16 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

---

[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.

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 Westerners 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 U.S. 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

---

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

[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.

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
- 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

---

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

[15] Ibid.

narrative and examine that narrative's content. The technology can help researchers focus while searching through massive amounts of social media data.

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.

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

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).

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?

Clint Watts
• Robert A. Fox Fellow, Foreign Policy Research Institute
• Senior Fellow, Center for Cyber and Homeland Security, the George Washington University

Statement Prepared for the U.S. Senate Committee on Armed Services – Subcommittee On Cybersecurity

"Cyber-enabled Information Operations" - 27 April 2017

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 30 March 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 U.S. 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

[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-for-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

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 manipulated 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.

[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

- ***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 U.S. 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 Russia'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, D.C. 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, D.C. 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.[56] The physical station or promotion

[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

of gray media outlets and overt Russian supporters in Eastern Europe were essential to their influence of the U.S. 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 émigré & associated offensive cyber operatives in U.S." during their recent campaign to influence the U.S. election. While still unverified, if true, employment of such agents of influence in the U.S. 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, U.S. 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, U.S. 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 U.S. 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.

---

[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

- **Task** – Witnessing the frightening possibility of Russian interference in the recent U.S. Presidential election, American policy makers have immediately called to counter Russian cyber influence. But the U.S. should take pause in rushing into such efforts. The U.S. and Europe lack a firm understanding of what is currently taking place. The U.S. 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 U.S. 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 U.S. 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 U.S. 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 U.S. 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

[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

and the bureaucracies America has created that prevent our country from employing its most talented cyber savants against the greatest enemies to our democracy.