Statement for the Record of
Dr. Mark R. Jacobson
Associate Teaching Professor
Edmund A. Walsh School of Foreign Service
Georgetown University

Before the
U.S. House of Representatives Committee on Science, Space, and Technology, Subcommittee on Oversight
Hearing entitled:
"Bolstering the Government's Cybersecurity: A Survey of Compliance with the DHS Directive"

November 14, 2017

Mr. Chairman, Ranking Member Beyer and distinguished members of the subcommittee. My name is Mark Jacobson, and I'm currently an Associate Teaching Professor at Georgetown University where I teach a number of courses in the Walsh School of Foreign Service. I've previously held several appointments at the Department of Defense and served as the first Deputy NATO Senior Civilian Representative in Afghanistan back in 2010-11. I'm also a former professional staff member at the U.S. Senate Committee on Armed Services. In addition to my civilian experience, I have had over twenty-three years as a reservist – in both the U.S. Army and U.S. Navy – and have mobilized twice on active duty, including to Afghanistan in 2006. I am also co-Author of a report entitled, *Shatter the House of Mirrors: A Conference Report on Russian Influence Operations*, and almost twenty years ago I was one of the first to address the problem of how the United States might respond pre-emptively or militarily to 'non-armed' subversive actions including cyber-attacks in an article entitled, *War in the Information Age: International Law, Self-Defense, and the Problem of 'Non-Armed' Attacks.* This challenge I note, remains with us today.

Thank you for the opportunity to appear before you to testify. I also wish to note that I am here today in my personal capacity and not representing any of my employers nor am I here as a member of the Navy Reserve or the Department of Defense.

My intent today is to try to help put the longstanding concerns that the U.S. government has had with Kaspersky Lab software into the larger foreign policy context. Cyber is, of course, but one arena for political, military, or economic action, albeit an incredibly powerful one. This committee is well aware of the dangers in the cyber-arena and the importance of strong cyber strategies, policies, and defenses in both the private and public sector. It is also difficult to overstate the imperative of "cyber hygiene." Without strong individual and group habits with regards to encryption, multi-factor authentication, password management, and the identification of phishing and similar online elicitation efforts, no cyber-security system will be effective.

In order, however, to fully understand the threats posed by viruses, back doors, or the type of front-door access that anti-virus companies like Kaspersky have, it is important to understand the overall objectives of the actors. In the case of nation-states, the nature of

their cyber activities is just a starting point as they are actions crafted to advance broader national foreign policy objectives. As you all know well, sometimes a cyber attack is simply an act of vandalism – to deface, annoy, or make an ideological point. Other times attacks are akin to more serious crimes such as robbery, blackmail, or the theft of intellectual property. Likewise, espionage is often the reason for cyber-intrusions into U.S. government and defense industry systems. I think we do a decent job of understanding these dynamics and activities – even if we cannot always totally prevent them.

What are of equal and sometimes greater worry for me are intrusions that are designed, in the end, to allow an actor to influence our attitudes and behaviors. Some intrusions may be designed to manipulate data. This is one of my greatest fears, especially considering the impact corrupt data that is believed to be accurate can have in the commercial, economic, and national security arenas. In short, manipulating data impacts our ability to understand what it is the data tells us, and not only can change our attitudes and perceptions but ultimately change our behaviors – perhaps leading us to make poor or even catastrophic decisions based on faulty raw data. Now imagine if manipulating data was part of an overall effort to influence our attitudes, perceptions, and behaviors. Imagine if data manipulation or obfuscation was coupled with public statements and news stories that supported that false narrative.

If there is but one thing to take away from my testimony today let it be that while cyber attacks and political warfare campaigns are a danger on their own, cyber-activities as part of an overall political warfare campaign are a particularly challenging threat, as they can prove incredibly effective at influencing attitudes and changing behaviors. Put another way, in political warfare campaigns and propaganda battles, it is the human mind that is the center of gravity.

It is worth noting that our adversaries have not hidden their intentions. For almost twenty-five years the Chinese have published the works of their military theorists in which the use of information warfare – which they believe will control the future of war – plays a central role in destroying an adversary's will and ability to fight. Similarly, in a doctrine that bears his name, the Russian Chief of the General Staff, General Valery Gerasimov, described that it was not effective for the Russians to match U.S. technological might, but rather to take an asymmetric approach and use a variety of information based tools, including the "use of technologies for influencing state structure and the population with the help of information networks."[1] These doctrines represent the digital equivalent of the age-old practice of political warfare and propaganda – efforts to create attitude and behavior change in a target audience. While cyber vulnerabilities can

[1] For a translation of the Gerasimov article describing his doctrine, see Robert Coalson's translation at https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian- non-linear-war/

also lead to attacks on infrastructure, the larger strategic vulnerabilities are in terms of the pathways it provides to wage influence campaigns targeting elected leaders, opinion-makers, or the population at large in the U.S. and other democracies.

Thus, my bottom line is that we need to consider that attempts to infiltrate U.S. government systems are part of broader efforts to advance the Russian foreign policy agenda. In other words, it's not just about the "hack" but also about what is being done to the data. Is an adversary copying the data to use it later as ammunition in a classic disinformation campaign, or is the data being corrupted so as to create a false impression? Indeed, might there be times where we even decide not to let them know they have been discovered?

As Dr. Jim Ludes, and I noted earlier this year in a co-authored report*, Shatter the House of Mirrors,* we must consider that Russia's well-financed and deliberate intervention in American political dialogue is part of a much broader effort to undermine America's faith in its free institutions and diminish U.S. political cohesion; erode confidence in western democracies and the credibility of western institutions; weaken trans-Atlantic relationships, including NATO; diminish the international appeal of the United States as well as reduce American power abroad.[2] In other words, we have to get beyond 2016 and think about U.S. national security more broadly rather than focusing on a single hack, one election cycle, or a single social media or anti-virus company.

As in any war, the Kremlin's objectives are political. The principal weapon in this conflict is information, and the evidence of Russia's use of it in Europe and the United States is clear. With the advent of ever-expanding and precise communications technologies capable of manipulating public opinion at the individual level on a massive scale – in particular social media - the tools and tactics of influence developed over the course of the 20th century can alter perceptions of reality to a degree that they can shape societies, influence election outcomes, and undermine states and alliances. Regardless of whether there is a relationship between Kapersky Labs and the Russian government or the software was simply vulnerable to a state-actor, that software becomes an entry point for espionage, propaganda operations, or subversion. Thus in defending against non-armed assaults in the information age, we must not forget to focus on the intentions and objectives of the political actor – whether the Russians, Chinese, or a range of terrorist or criminal networks.

"What's Past Is Prologue"

The good news – propaganda and political warfare campaigns are not new. They are as old as the Bible and there are a variety of ways in which we can combat it and mitigate the consequences. It is worth noting that just over 500 years ago Martin Luther's "95 Theses" were promoted through the Twitter of his day. In this case the printing press combined with a variety of social networks allowed his message of religious reform to go "viral." As his friend Freidrich Myconius would note, "hardly 14 days had passed when

[2] James M. Ludes, PhD and Mark R. Jacobson, PhD, *Shatter the House of Mirrors: A Conference Report on Russian Influence Operations,* Salve Regina University, Pell Center for International Relations

these propositions were known throughout Germany and within four weeks almost all of Christendom was familiar with them."[3]Today, of course, those timelines might read 14 minutes and four hours.

The history of the Cold War provides us with an even better guide to how the Russians might use what was termed "active measures," or, political subversion, sabotage and information operations, including disinformation.[4] For the United States, these measures short of war, known as "political warfare" and encompassing both overt and covert operations were the most effective means to pressure the Soviet Union without risking a general conflict. For the United States, the emphasis was on engagement with the Soviet people and a strategy of exposing the truth and rot of the Soviet system in the hopes that the system would collapse from within. The Soviets also sought to expose flaws in the American system, notably the racial divide; but Moscow also sought to manufacture and spread deliberate disinformation about America. Going even further, these propaganda efforts were supported by subversive activities such as the Teacher's Riots in Japan in 1960 and an attack on Vice President Richard Nixon's convoy in Venezuela in 1958.

Even more dramatic efforts came in 1983, when Soviet intelligence operatives spread a "fake news" story with a pro-Soviet Indian newspaper alleging that the AIDS virus was developed by the U.S. government to target African-Americans and the homosexual community. Within four years the story had been repeated in the Soviet Union and in outlets in over 80 countries and in 30 languages.[5] The story did tremendous damage to U.S. credibility abroad as well as at home. At least one study as late as 2005 found that almost 50 percent of African-Americans believed that HIV was a "man-made virus" designed to wipe out the African-American community.[6]

As noted in our report, this was not the first Russian effort to stoke racial tensions and efforts to do so reached the heart of the Civil Rights movement:

> At the height of the civil rights movement, Soviet intelligence first sought to discredit Martin Luther King Jr. because he preached racial reconciliation. The Soviets favored instead more militant African-American activists who might provoke a full-blown race war in the United States. Towards that end, the Soviets generated a propaganda campaign to depict King as a collaborator with white oppressors. After his assassination, however, Soviet propaganda

---

[3] Margrethe Vestager, "Luther and the Modern World" Speech to the 9th Luther Conference, Copenhagen, 2016. Available at: https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/luther-and-modern-world_en

[4] The following paragraphs are adapted from Ludes and Jacobson, *Shatter the House of Mirrors.*

[5] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," INSS Strategic Perspectives No. 11, June 2012.http://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf

[6] Darryl Fears, "Study: Many Blacks Cite AIDS Conspiracy," *Washington Post*, January 25, 2005, http://www.washingtonpost.com/wp-dyn/articles/A33695-2005Jan24.html?tid=a_inl

targeting the African-American community portrayed King as a martyr and sought to enflame the passions of the community already rioting in American cities.[7]

This was prologue for much of what we have seen in recent months and what we can expect to see in the future – divisive propaganda designed to exploit divisions in our country over race, guns, and LGBTQ rights – anything where they can drive those with different views to extremes. Clearly the Russians did not create the issues that cause division in the United States, but they are exploiting them and exacerbating the problems. Russia will overtly and covertly support organizations seeking secession or seeking to politically divide the United States and they will covertly press protest movements to move towards the extreme and ultimately violence, just as they did during the Cold War.

With so much of American political dialogue taking place over social media and with 67% of Americans receiving at least some of their news over social media it is not surprising that this platform has become a target for its Russian agents as well as their bots and trolls in an effort to create trends and increase the popularity of false narratives. The fingerprints of Russian government sponsored disinformation campaigns have been left on the Russian parliamentary election of 2011 and during the Scottish independence referendum of 2014, and there is some evidence of a Russian hand during the debate over "Brexit." I suspect we will see echoes of Russian involvement in the Catalonian independence movement and as seen in recent hearings on Capitol Hill. Russian social media propaganda still infects Twitter, Facebook and other U.S. based social media outlets and only now are we beginning to understand Chinese influence operations via these same platforms.[8]

So What Do We Do?

So what do we do about this? As I noted earlier in my testimony, in these battles to influence and persuade it is the human mind that is the center of gravity. We must think about how to strengthen the public's ability to interact with the information that it sees in a digital world.

In particular, we need to play to our strengths as a nation and perhaps our greatest strength is our belief in the free-exchange of information and the freedom of expression. Even when we disagree vehemently it is dialogue and discussion that will help bring transparency when actors seek to opacity. This may mean changes to the norms and potentially the regulations that govern social media. While we must respect the business model of the social media platforms, the social media companies must do more to combat

---

[7] Christopher Andrew and Vasili Mitrokhin, *The Sword and the Shield,* (New York: Perseus Books, 1999), 237-238.

[8] Mark Jacobson, "Target America: Dissecting Moscow's Social Media Campaign," *The Cipher Brief, October 31, 2017*. https://www.thecipherbrief.com/target-america-dissecting-moscows-social-media-campaign. On Chinese propaganda efforts see, "China Spreads Propaganda to U.S. on Facebook, a Platform It Bans at Home," *The New York Times,* November 8, 2017, available at https://www.nytimes.com/2017/11/08/technology/china-facebook.html

hate speech and weed out extremism as well as accept that they are as much "media" as they are "social." Accordingly, political advertisements on these platforms should face the same regulation they do in the print and broadcast arenas.

There may be need for changes in the traditional news arena as well. Even the most professional news organizations can be taken in by fabricated stories; the traditional news media may need to consider whether their current professional standards and practices allow them to identify when they have become a vehicle for a propaganda campaign.

Most importantly, we, as a nation must begin a concerted effort to properly educate the American public about the disinformation campaigns they face in the world today. It is critical we inoculate against the viral threat of disinformation through more education and training in the art of media literacy. Children and adults alike must be able to differentiate between advertisements and news articles and learn how to identify the source of information they find on the Internet. This will require significant efforts at the K-12 level in order to help students avoid falling prey to "fake news." While disheartening, it is important to note the findings of the Stanford History Education Group in recent reporting. Not only is it easy to "dupe" middle school, high school, and college students online, but also "experts" often fell victim to "easily manipulated features of websites, such as official-looking logos and domain names."[9] The silver lining in this report, however, was that trained fact-checkers did much better at correctly identifying legitimate sources and evaluating information. If we give our students and public the tools, they can do a great deal on their own to address this challenge.

Finally, the ability to evaluate information, think critically, maintain a healthy skepticism, and understand that some messages out there are deliberately deceptive will make our population much more conscious about the information they absorb. Likewise, it is the cornerstone of civic literacy – something that is sorely lacking in our toolboxes today. These educational imperatives are not easy tasks and it may require the same level of effort as seen with President Eisenhower's National Defense Education Act of 1958 – an attempt to bolster poor American efforts in terms of math, science, and foreign language education. Just as Eisenhower believed those skills were critical to keep pace with the national security threats in the post-Sputnik era; media, civic, and historic literacy alongside critical thinking may be what is needed to protect our freedoms today.

At the risk of sounding too professorial, I think it is important to conclude by reminding the committee of two letters that Mark Twain sent to celebrate the opening of the Gutenberg Museum in 1900. In them Twain reminded the world that Gutenberg's printing press was "incomparably the mightiest event" in history but brought with it not only a "new and wonderful earth" but a "new hell." Twain eloquently recounted the details, developments, and marvels that the new form of communication brought:

> It found Truth walking, and gave it a pair of wings; it found Falsehood trotting, and gave it two pair. It found Science hiding in corners and hunted; it has given it the freedom of

[9] Chronicle of Higher Education, *Teaching Newsletter: One Way to Fight Fake News*, November 9, 2017.

> the land, the seas, and the skies, and made it the world's welcome quest. It found the arts and occupations few, it multiplies them every year…It has set people's free, and other peoples it has enslaved; it is the father and protector of human liberty, and has made despotisms possible where they were not possible before.[10]

In short, Twain wrote, "what the world is today, good and bad, it owes to Gutenberg."

The Internet revolution may surpass Gutenberg's printing press as the "greatest event" in secular history – and yes, has already created new and wonderful opportunities and a plethora of wicked challenges. It may be used for good and for bad. In the end, however, it is used by human beings. The human dynamic, human intentions, and human solutions must remain at the forefront of our understanding of the problems and policy solutions.

[10] Mark Twain, Letter to the *Hartford Daily Courant*, June 27, 1900 and letter to the *Gutenberg-fest-zu-Mainz im jahre 1900*, 1901. Available at: http://www.twainquotes.com/Gutenberg.html