



March 30, 2017

# Disinformation: A Primer in Russian Active Measures and Influence Campaigns

Select Committee on Intelligence, United States Senate, One Hundred  
Fifteenth Congress, First Session

---

## HEARING CONTENTS:

### Witnesses

Eugene Rumer  
Director  
Russia and Eurasia Program, Carnegie Endowment for International Peace  
[View Testimony](#)

Roy Godson  
Professor of Government Emeritus  
Georgetown University  
[View Testimony](#)

Clint Watts  
Senior Fellow  
Foreign Policy Research Institute Program on National Security  
[View Testimony](#)

Kevin Mandia  
CEO  
FireEye  
[View Testimony](#)

*\* 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.*

---



Keith Alexander  
CEO and President  
IronNet Cybersecurity  
[View Testimony](#)

Thomas Rid  
Professor, Department of War Studies  
King's College London  
[View Testimony](#)

**Compiled From\*:**

<https://www.intelligence.senate.gov/hearings/open-hearing-disinformation-primer-russian-active-measures-and-influence-campaigns>

<https://www.intelligence.senate.gov/hearings/open-hearing-intelligence-matters-1>

*\* 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.*

---



**CARNEGIE**  
ENDOWMENT FOR  
INTERNATIONAL PEACE

---

**Congressional Testimony**

---

**RUSSIAN ACTIVE MEASURES AND  
INFLUENCE CAMPAIGNS**

**Eugene B. Rumer**

Senior Fellow and Director

Russia and Eurasia Program

Carnegie Endowment for International Peace

Testimony before U.S. Senate Select Committee  
on Intelligence

March 30, 2017

Chairman Burr, Vice Chairman Warner, distinguished members of Senate Select Committee on Intelligence!

It is a great honor to appear here today. The issue before this panel is Russian active measures and influence campaigns. It rose to the top of our national agenda in 2016, when we became aware of Russian interference in our presidential campaign. It remains one of the most contentious issues in our national conversation, for the very idea that another nation could put at risk the integrity of our country's most essential institution—the process of electing our president—is hard for us to comprehend.

I would like to state at the outset that based on media reporting, on statements of senior [U.S.](#) and [other countries'](#) law enforcement and intelligence officials, and my professional experience as a student of Russian foreign policy, I am convinced that Russian intelligence services, their proxies, and other related actors directly intervened in our election in 2016.

You might ask why I am so confident of this. I have not seen the classified evidence that supports the findings presented in the Intelligence Community Assessment “[Assessing Russian Activities and Intentions in Recent US Elections](#)” published by the Office of the Director of National Intelligence on January 6, 2017. Some observers have been critical of that Assessment for not presenting detailed evidence of Russian cyber intrusions or covert activities. They miss the mark—it is the totality of the Russian effort to interfere, mislead, misinform, outright falsify, influence, etc. that is just as, if not more convincing than the cyber evidence of the Russian break in into the Democratic National Committee (DNC) server and other intrusions. That Russian effort is before us in plain sight—in state-sponsored propaganda broadcasts on RT (Russia Today), in countless internet trolls, fake or distorted news spread by fake news services, in the recent [Kremlin get together](#) of Russian president Vladimir Putin with the French far right presidential candidate Marine Le Pen. The list can go on. That effort is also an integral part of Russian foreign policy and domestic politics.

### *It's More than the Economy*

To understand why the Russian government is engaged in this large-scale and diversified influence operation, which blends overt and covert activities, one needs to step back and put it in the context of events of the quarter century since the end of the Cold War.

Every country's foreign policy is a product of its history, its geography, and its politics. Russia is no exception to this rule, and to understand the pattern of Russian behavior at home and abroad, we need to look at Russian history, Russian geography, and Russian domestic politics.

War in Europe is integral to the formative experience of every Russian. The country's national narrative is impossible without the record of two wars—the Patriotic War of 1812, which Russians view as a war of liberation from Napoleon's invasion of Russia, and the Great Patriotic War of 1941-1945. Both wars were fought to liberate Patria, the Fatherland, from foreign occupiers. In 1812, Napoleon entered Moscow and the city was burned. In 1941, Hitler's armies were stopped

just outside the city limits of Moscow. Americans, too, had their war of 1812, and Washington too was burned, but few Russians know or remember it, just as they think little of the fighting in the Pacific theater against Japan in the second world war. Stalin's armies didn't enter it until nearly the very end, three months after the war in Europe ended. The end of the Great Patriotic War is celebrated in Russia every year as a great national holiday on May 9. The greatest Russian novel of all times is Leo Tolstoy's *War and Peace*, all Russians read it in high school. They are also taught in history classes that their country's greatest accomplishment of the 20th century was the defeat of fascism in the Great Patriotic War.

The war of 1812 ended for Russia when the armies of Tsar Alexander I entered Paris in 1814. The Great Patriotic War ended in 1945 when Stalin's armies entered Berlin. From 1945 to 1989, when the Berlin Wall came down, Russia was at its most secure, or so successive generations of Russian leaders have been taught to believe. The history and the strategy taught in Russian military academies for decades after it ended were the history and the strategy of the Great Patriotic War. The map for tabletop exercises at the Military Academy of the General Staff in 2001 was a giant map of the European theater. U.S. strategists were by that time "done" with Europe and shifting their focus from the Balkan edge of the continent to South Asia and the Middle East. Russia was not "done" with Europe.

Little appreciated in the West at the time was the trauma suffered by the Russian national security establishment when it lost its outer and inner security buffers—the Warsaw Pact and the Soviet empire. The sense of physical security afforded by this dual buffer between NATO's armies and the Russian heartland was gone. Russian declaratory policy may have been to sign on to the 1990 [Charter of Paris](#) as the Cold War ended, but the historical legacy and the geography of Russian national security could not be altered with the stroke of a pen. Even as the Communist system was dismantled and the Soviet Union disbanded, Russia's national security establishment, which had been brought up for generations to think in terms of hard power, could not and did not embrace the new vision of European security based on shared values.

In 1991, with their society in turmoil, their economy in tatters, their military in retreat from the outer and inner empires, and their country literally falling apart, Russian leaders had no choice but to go along with that vision. They also accepted as given that history is written by the victors, and that the victors would also make the rules for the new era. Russia would have to go along with it for as long as it remained weak.

The 1990s were a terrible decade for Russia. Its domestic politics remained in turmoil, its economy limped from one crisis to the next, and its international standing—only recently that of a superpower—collapsed. Western students of Russia were entertaining the prospect of a [world without Russia](#). It was not lost on Russian political elites that the 1990s were also a time of great prosperity and global influence for the West. For them, brought up on the idea of importance of hard power, the dominance of the West was inextricably tied to its victory in the Cold War, the defeat of Russia, its retreat from the world stage, and the expansion of the West in its wake.

## *Russia Is Back*

But Russia would not remain weak indefinitely. Its economic recovery after the turn of the century, buoyed by soaring global prices for commodities and hydrocarbons, and its domestic political consolidation around Vladimir Putin and his brand of increasingly authoritarian leadership, so different from the leadership of Boris Yeltsin, have laid the groundwork for a return to Russia's more assertive posture on the world stage.

That increasingly assertive posture has manifested itself on multiple occasions and in different forms over the past decade and a half—in Vladimir Putin's [speech](#) at the Munich Security Conference in 2007; in the war with Georgia in 2008 and the statement in its aftermath by then-president Dmitry Medvedev about Russia's claim to a sphere of "[privileged interests](#)" around its periphery; and finally in the annexation of Crimea in 2014 and the undeclared war in eastern Ukraine to keep Ukraine from slipping from Russia's orbit.

For the West, Russia's return to the world stage has been nothing more than pure revanchism. It violates the basic, core principles of the post-Cold War European security architecture—which Russia pledged to observe over a quarter-century ago.

For Russia, it is restoring a balance—not the old balance, but some semblance of it. Currently, NATO troops are deployed to deter Russian aggression against Estonia. (Curiously, former speaker of the House Newt Gingrich has described it as the "[suburbs of St. Petersburg](#).”) Russia's security establishment views this commitment by NATO countries to its vulnerable ally as a threat to the heartland.

The narrative of restoring the balance, correcting the injustice and the distortions of the 1990s, when the West took advantage of Russia's weakness, has been the essential element of Russian state-sponsored propaganda since the beginning of the Putin era. Whether or not we choose to accept this narrative, these beliefs undergird Russia's comeback on the world stage and political consolidation at home. In public and private, top Russian officials proclaim that the wars in Georgia and Ukraine were fought to prevent Western encroachment on territories vital to Russian security. The military deployment in Syria merely restores Russia's traditional foothold in the Middle East, from which Russia withdrew when it was weak, and where it was replaced by the West with consequences that have been tragic for the entire region.

In domestic politics, Putin's authoritarian restoration is treated by the majority of average and elite members of Russian society as the return to the country's traditional political health, free from foreign interference in its political and economic life. The more pluralistic system and dramatic decline of the 1990s are linked in this narrative to the influence of the United States and other foreign interests in Russia's economy and politics, to their desire to introduce alien values in Russia's political culture and take Russia's oil. U.S. support for Russian civil society is an effort to undermine the Russian state, to bring Russia back to its knees, and take advantage of it, both at home and abroad. Western economic sanctions imposed on Russia in the wake of its annexation of Crimea and the undeclared war in eastern Ukraine are a form of warfare designed to weaken

Russia and gain unfair advantage over it. Western support for democracy in countries around Russia's periphery is an effort to encircle it and weaken it too.

This narrative has dominated the airwaves inside Russia, where the Kremlin controls the television, which is the principal medium that delivers news to most Russians. With independent media in retreat and alternative sources of information marginalized, this narrative has struck a responsive chord with many Russians. The narrative has been effective because it contains an element of truth—Russia did implode in the 1990s, and the West prospered; Russia did recover from its troubles and regained a measure of its global standing on Putin's watch; the West did promote democracy in Russia, which coincided with its time of troubles; and the West has been critical of the Russian government's retreat from democracy as Russia regained strength.

Moreover, foreign policy traditionally was and is the preserve of the country's political elite and its small national security establishment. Whereas there are some voices inside Russia who, like the leading anti-corruption activist Alexei Navalny, have challenged the many domestic failings and authoritarian leanings of the Putin government, there are hardly any who have challenged its foreign policy record. Worse yet, the Kremlin propaganda has been apparently so effective, and the legal constraints imposed by it so severe, that few Russian opposition voices dare to challenge the government's foreign policy course for fear of being branded as foreign agents, enemies of the people, and fifth columnists.

### *Warfare by Other Means*

For all the talk about Russian recovery and resurgence on the world stage, its capabilities should not be overestimated. Its GDP is about \$1.3 trillion vs. U.S. GDP of over \$18 trillion. The Russian economy is not "in shambles," but in the words of a leading Russian government economist it is doomed to "eternal stagnation" unless the government undertakes major new reforms.

Russian defense expenditures are *estimated* at about \$65 billion, or little more than President Trump's proposed increase in U.S. defense spending for FY 2018. The Russian military is *estimated* at just over 750,000—well short of its authorized strength of *one million*—vs. U.S. 1.4 million active duty military personnel.

By all accounts, the Russian military has made huge strides in the past decade, benefiting from far-reaching reforms and generous defense spending. It is undeniably far superior militarily to its smaller, weaker neighbors and enjoys considerable geographic advantages in theaters around its periphery.

Yet, the overall military balance does not favor Russia when it is compared to the United States and its NATO allies. They have bigger economies, spend more on defense, have bigger, better equipped militaries, and are more technologically sophisticated. A NATO-Russia war would be an act of mutual suicide, and the Kremlin is not ready for it. Its campaign against the West has to be prosecuted by other means.

That is the backdrop for the subject of today's hearings. Since Russia cannot compete toe-to-toe with the West, its leaders have embraced a wide range of tools—information warfare in all its forms, including subversion, deception, dis- and mis-information, intimidation, espionage, economic tools, including sanctions, bribery, selective favorable trading regimes, influence campaigns, etc. This toolkit has deep historical roots in the Soviet era and performs the function of the equalizer that in the eyes of the Kremlin is intended to make up for Russia's weakness vis-à-vis the West.

In employing this toolkit, the Kremlin has a number of important advantages. There is no domestic audience before which it has to account for its actions abroad. The Kremlin has few, if any external restraints in employing it, and its decisionmaking mechanism is streamlined. There is no legislature to report to, for the Duma is a rubber stamp body eager to sign off on any Kremlin foreign policy initiative.

The circle of deciders is far smaller than the Soviet-era Politburo, and it is limited to a handful of Putin associates with similar worldviews and backgrounds. They are determined to carry on an adversarial relationship with the West. They can make decisions quickly and have considerable resources at their disposal, especially given the relatively inexpensive nature of most of the tools they rely on. A handful of cyber criminals cost a lot less than an armored brigade and can cause a great deal more damage with much smaller risks.

Shame and reputational risks do not appear to be a factor in Russian decision-making. In early-2016, Russian Foreign Minister Sergei Lavrov did not shy away from [repeating](#) a patently false fake media story about the rape of a Russian-German girl by a Syrian asylum-seeker in Germany.

Moreover, a version of selective naming and shaming—or targeting of political adversaries with false allegations of misconduct—has been used by Russian propaganda to discredit political adversaries in the West. Russian propaganda, and [Putin](#) personally, have sought to deflect the attention from the fact of the intrusion into the DNC server and the top leadership of Hillary Clinton's presidential campaign to the information released as a result of it that has presented various political operatives in an unfavorable light.

This not only deflects the attention from Russia's role in this episode, it helps the Kremlin convey an important message to its domestic audience about the corrupt nature of U.S. politics. Russia therefore is no worse than the United States, which has no right to complain about corruption and democracy deficit in Russia.

Russian meddling in the 2016 U.S. presidential election is likely to be seen by the Kremlin as a major success regardless of whether its initial goal was to help advance the Trump candidacy. The payoff includes, but is not limited to a major political disruption in the United States, which has been distracted from many strategic pursuits; the standing of the United States and its leadership in the world have been damaged; it has become a common theme in the narrative of many leading commentators that from the pillar of stability of the international liberal order the United States has been transformed into its biggest source of instability; U.S. commitments to key allies in Europe and Asia have been questioned on both sides of the Atlantic and the Pacific. And last, but

not least, the Kremlin has demonstrated what it can do to the world's sole remaining global superpower.

*It Is Not a Crisis, It Is the New Normal*

Events of the past three years, since the annexation of Crimea by Russia, have been referred to as a crisis in relations between Russia and the West. However, this is no longer a crisis. The differences between Russia and the West are profound and are highly unlikely to be resolved in the foreseeable future without one or the other side capitulating. The U.S.-Russian relationship is fundamentally broken, and this situation should be treated as the new normal rather than an exceptional period in our relations. For the foreseeable future our relationship is likely to remain competitive and, at times, adversarial.

The full extent of Russian meddling in the 2016 presidential election is not yet publicly known. But the melding of various tools (e.g. the use of cyber operations to collect certain information covertly) and the provision of this information to outlets such as Wikileaks and the news media was certainly a first. Unfortunately, it is not a first for U.S. allies and partners in Europe and Eurasia. It is not the last either. Just a few days ago, Vladimir Putin received France's right-wing presidential candidate Marine Le Pen in the Kremlin. Previously, her National Front had [received](#) a loan from a Moscow-based bank, and Russian media outlets have tried to injure the reputation of her chief opponent Emmanuel Macron by spreading [rumors](#) about his sexuality and ties to financial institutions. The chiefs of [British](#) and [German](#) intelligence services have warned publicly about the threat from Russia to their countries' democratic processes. The Netherlands recently [chose](#) to forego reliance on certain computer vote tabulation systems due to elevated fears of Russian interference and hacking.

The experience of Russian meddling in the 2016 U.S. election should be judged an unqualified success for the Kremlin. It has cost it little and paid off in more ways than can be easily counted. To be sure, U.S. officials should expect it to be repeated again and again in the future. 2016 was a crisis, but it was not an aberration and should be treated as the new normal. Cyber is merely a new domain. Deception and active measures in all their incarnations have long been and will remain a staple of Russia's dealings with the outside world for the foreseeable future.

**Written Testimony of ROY GODSON to the  
Senate Select Committee on Intelligence, Open Hearing, March 30, 2017  
“Disinformation: A Primer in Russian Active Measures and Influence  
Campaigns.”**

Thank you Chairman Burr and Vice Chairman Warner for the opportunity to testify today on Russian Active Measures and Influence Campaigns.

My name is Roy Godson, and I am Emeritus Professor of Government at Georgetown University.

Active Measures (AM) have been a significant weapon in the Russian and Soviet arsenal for over 100 years. By active measures is meant the coordinated direction by the centralized authoritarian hierarchy of a combination of overt and covert techniques that propagate Russian, (formerly Soviet) ideas, political/military preferences and undermine those of their democratic adversaries. Disinformation – intentionally disseminating false information such as forgeries - is just one of the many overt and covert influence techniques used by the Russian/Soviet leadership in what they call “active measures.”<sup>1</sup> A more comprehensive definition is offered at the end of this statement.

There is little new in the basic mindset of successive generations of Russian leadership. These influence techniques provide their relatively weak economy and insecure political institutions with a strategic and tactical advantage to affect significant political outcomes abroad. ***They say so. They do it.*** But they are not ten feet tall. They build up skilled, experienced, and tenacious teams at home in their government and quasi-government agencies. They maintain and develop both an overt and covert apparatus of well-trained personnel to continue their manipulation of foreign agents of influence, and use new geotechnologies that come online as force enhancers. Some of it is effective, some just a nuisance.

---

<sup>1</sup> For a brief listing of major active measures techniques, See, Richard Shultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy*, Pergamon-Brassey’s, 1984.

In the final years of the Soviet Union there was enough information on their active measures systems to conclude that approximately 15,000 personnel and several billions of hard currency annually were being spent on these activities— aimed mostly at the U.S. and its allies.

Yet even with knowledge of these activities and their long-term training of personnel, as well as studies by Western scholars, information from former Soviet defectors in the active measures “industry,” the attentive public and most elected officials still continue to be surprised by Russia’s operational behavior.

Recent events are not the first time we have been SURPRISED.

### **Punching Above Their Weight**

After World War I, a few Americans and others had warned about these “below the radar” threats. Some were veterans of the internecine wars during and after the Bolshevik Revolution and were aware of the Communist “ways” of politics. They also reported that Lenin and Stalin had already started to build up the capability—since encompassed by the term “Active Measures”—in the Twenties to defend the Revolution and to influence world politics. The Soviet Politburo and the Party departments directed, controlled, and financed active measures and serviced them through the Soviet intelligence system and Soviet diplomacy. These instruments and capability provided influence throughout the world to the economically weak Soviet regime along with its faithful allies inside most of the democratic (and illiberal) societies—from the 1930s to the early 1990s.

Moscow reinforced its sway by creating and controlling an apparently independent mostly overt grouping of the Communist parties known as the Communist International. This International, in turn, was bolstered by another set of organized national and international Front groups, again apparently independent of Soviet control. These “nongovernmental” Fronts were designed to appeal to non-communists and political activists who were attracted or amenable to Soviet views in specific sectors such as “labor,” “youth,” “peace,” “religion,” and “culture.” The Parties and Fronts changed their views and their tactics in response to Moscow’s direction, working, for example, against the Nazi and Fascist rise to power in Europe in the 1930s until 1939.

Then, after the Hitler-Stalin Non-Aggression Pact in 1939, which divided Poland in two and enabled Moscow to consolidate control the Baltic States, Stalin switched policies. No longer did Communists parties and fronts work against the Nazis. Instead they condemned “capitalist liberals” and sought to influence and undermine the political system in the West. Stalinist policy flipped again when Germany attacked Russia in 1941, and for the rest of the war the Russians mobilized the Communist parties and the Fronts to support the Soviet Union in the war effort and take over the then anti-Nazi Resistance in Europe.

They used this Resistance role to gain spectacular influence in postwar European politics, particularly in France and Italy, and almost in West Germany as well as in Britain and other countries. The Communist Parties and fronts also helped – overtly and covertly- in recruiting agents of influence, and some Western leaders and voters, who had become sympathetic to the anti-Nazi and Fascist positions of the Soviet Union, and the peace movements and other issue organizations that the Soviets significantly influenced. An extensive academic, journalistic, and biographic literature is now available on these efforts.<sup>2</sup>

Little evidence has come to the fore of Soviet direct meddling in the actual mechanical election processes of major countries; but they did try to influence the outcomes of the elections and the behavior of foreign leaders in parties, trade unions, the media, and culture. Sometimes they were successful, sometimes less so. While leaders of democratic governments came to be generally aware of Soviet influence attempts, they rarely attracted the ire and response of the United States until later. Nevertheless, using their broad active measures capability, in the post WWII context, the Soviets almost succeeded in shifting the entire postwar political balance of power in Western Europe.

### **A Closely Fought Battle**

This strategic capability went almost unnoticed during WWII and the first years afterwards. But gradually, the scope of long-term Soviet penetration and active measures in Europe, and the United States, came into focus – and to public attention. The battle for political power in post-

---

<sup>2</sup> See for example, Haynes, John Earl, Harvey Klehr, and Alexander Vassiliev. 2010. *Spies: The Rise and Fall of the KGB in America*. Yale University Press. See also, Godson, Roy, *American Labor and European Politics, The AFL as Transnational Force*, Crane, Russak, 1976. Shultz and Godson, *Dezinformatsia*.

war Western Europe – then the pivot of world politics – galvanized U.S. action at home and abroad. It was a formidable response.

The Truman and Eisenhower administrations developed a national “whole of government” and “whole of society” political strategy to neutralize Soviet active measures from the late 1940s on. This was a calculation to partially complement both U.S. foreign economic policy (e.g. The Marshall Plan) and its military strategy (e.g. NATO). Initially, there was a good deal of improvisation. Gradually, however the bipartisan political leadership, the Executive Branch, and Congress, together with the support of the private sector, labor, and philanthropy, and education were awakened to the threat and mobilized in support. There were, of course, American mistakes, and some demagoguery – especially in the early 1950s from Senator Joseph McCarthy and his team who exploited public concern, exaggerated the danger, and overreacted.

Yes, from the late 1940s forward the U.S. and other liberal democracies did use overt and covert measures to defend and assist democratic elements abroad—labor, media, intellectuals, and parties—that were under direct attack abroad by well-trained and financed political forces from the Soviet Bloc.

By the late 1960s the political consensus in the U.S. and to some extent among democratic allies abroad began to fray, particularly during the Vietnam War. The coalition of American liberals and conservatives against Soviet active measures came apart. Congressional criticism of the intelligence community and the dismantling of much of the U.S. capability to counter Active Measures abroad also contributed.

Also in the 1970s, the Nixon Administration began to seek “Détente” with the USSR and that too diminished government support for exposing and criticizing Soviet active measures abroad. By the advent of the Carter Administration in the mid-1970s, interest in and the ability to counter Soviet influence operations abroad had waned substantially.

That changed when we were “surprised” again —this time by the Soviet invasion of its neighbor Afghanistan, Soviet support for Cuban expeditions in Africa, the Sandinista takeover of Nicaragua and the threat to El Salvador. This was intensified by the Soviet build-up of warfighting capabilities aimed at Western Europe and vigorous Soviet active measures

campaigns there – with the goal of minimizing the NATO response.<sup>3</sup> Even before Reagan took office in 1981 awareness of the importance of a response was growing in Washington.

Fortunately, U.S. government capabilities had not been entirely dismantled in the 1970s. There were still a few veteran specialists in the USG – State, CIA, DOD, DIA, and the then USIA, as well as some in Congress – who had maintained a watching brief on the issues. They were complemented by American NGOs such as the mainstream of organized labor and key philanthropic and human rights organizations who had sustained attention and enquiry on Soviet active measures. Once again, plans to counter Soviet Active Measures were reprised, first with educational campaigns and then with significant tangible support to democratic elements at home and abroad.

After a brief interlude in the Yeltsin years of the 1990s and the demise of both the Soviet Communist Party and its ideology of Marxism Leninism, the regime regrouped this time under the leadership of Vladimir Putin. He came to power together with a coterie of former colleagues, many also trained in the Soviet security and intelligence system. They no longer had a competitive global ideology, and much of their widespread apparatus such as Communist Parties and Front groups was not particularly useful. What they did share with their predecessors was an animosity toward liberal democracy.

They were and are determined to achieve most of the same objectives as the Soviet Communist Party leadership had had before them. As determined Russian nationalists they sought power and influence, and, of course, discrediting the U.S. and democratic society in general. Their focus is almost completely negative, zeroing in on creating chaos and division in what has been called an “age of anger” in many parts of the world.<sup>4</sup> This opens up many opportunities for influence.

Their active measures apparatus appears to still recruit and train operatives for the global context. They identify and pursue opportunities as they see them. They still use a combination (Kombinatsia) of overt and covert techniques that date back to Czarist days to reinforce their medium to long-term objectives. Of course, they have taken advantage of the new advances in

---

<sup>3</sup> Godson Roy, *Dirty Tricks or Trump Cards: U.S. Covert Action and Counterintelligence*, Transaction, 2000.

<sup>4</sup> Mishra, Pankaj. *Age of Anger: A History of the Present*. New York: Farrar, Straus and Giroux, 2017. See also Friedman Thomas L. *Thank You for Being Late: An Optimist's Guide to Thriving in the Age of Accelerations*, Farrar, Straus and Giroux, 2016

global technologies, most notably the Internet and new media<sup>5</sup> – and are also likely pursuing other geotechnologies coming on stream soon.<sup>6</sup>

As one student of the subject has put it, “they are mixing old and new wine in new bottles — but the distributor is basically the same.”

### **The U.S. Response in the 1980s**

The U.S. government began to develop a strategic approach to the problem by mobilizing an interagency effort in the early Reagan years. This difficult and complex task took time and effort. The various departments and agencies concerned with national security slowly began to pull together to provide details to the American people about Soviet activities designed to influence American and allied politics.

Achieving this synergy required that the President request and receive support from the Congress to authorize and fund more gathering of information from overt and intelligence sources about the specifics of Soviet AM, and to analyze and even to anticipate their likely future operations. It was reinforced by the creation of what came to be known as the interagency “Active Measures Working Group,” based first in the State Department and later in the U.S. information Agency.<sup>7</sup> Some of the findings were used to educate Americans, Europeans, and others that Moscow was conducting major campaigns to discredit democracy in general, and the U.S. in particular,

As a result, countering Soviet active measures became a government concern and an issue in Washington and then in U.S. Embassies abroad. This also coincided with both Congressional and educational, and media interest in the subject. Newspapers, journals, books, and television reported on the subject. Although at first disparaged, *Dezinformatsia* —Disinformation, and *Aktivniye meropriyatiya*—Active Measures, and *Kombinatzia* — employing both overt and

---

<sup>5</sup> Office of the Director of National Intelligence, “Assessing Russian Activities and Intentions in Recent U.S. Elections,” ICA 2017-01D, 6 January 2017.

<sup>6</sup> There is however, a dearth of public information of this subject.

<sup>7</sup> Fletcher Schoen and Christopher J. Lamb, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made A Major Difference*, Center for Strategic Research, Institute for National Strategic Studies, National Defense University, 2012.

covert techniques—entered into the lexicon in policy and academic circles,<sup>8</sup> much as *Kompromat* or compromising material has today.

The second result of the Soviet active measures in this period was to help stimulate the Administration and the Congress to actively promote abroad positive liberal principles and institutions, particularly electoral democracy, the rule of law, and human rights. Active involvement by the U.S. in the positive promotion of liberal principles had waxed and waned throughout the 20<sup>th</sup> Century. It now blossomed again. The U.S. did this unilaterally as well as in partnership with Allies and global and regional organizations. In part this was because the principles were considered part of the American heritage. But it was also because the U.S. had security interests in supporting democratic forces abroad who were competing with communism and Soviet influence, as well as with other illiberal actors such as organized crime and kleptocracy.

An outstanding example was the creation and continuation of bipartisan support and funding of what became the National Endowment for Democracy in 1984. It was focused on helping to support electoral democratic principles abroad. There were many other “whole of government” efforts to entertain smaller but sometimes effective projects, on religious freedom and toleration, and human rights.

It is difficult to assess the overall effectiveness of these efforts. There has been some evaluation of the U.S. performance. Some well-informed practitioners maintain that they were a major cause of the demise of the USSR – that it stimulated the final collapse of the Soviet system in Russia and Central and Eastern Europe.<sup>9</sup> Academics in particular tend to believe that there were multiple long and short-term causes of how and why the Soviet Union disintegrated.

But it happened, and as Americans have been wont to do after other successes abroad, interest in the competition between liberal and illiberal actors in world politics waned – as it had after World War I and World War II. After a few years at the turn of the 20<sup>th</sup> Century, illiberal actors in Russia regained control of the country with much of its active measures apparatus intact. In the main, we were again surprised.

---

<sup>8</sup> Richard Shultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy*.

<sup>9</sup> See for example, Kraemer, Sven F, *Inside the Cold War from Marx to Reagan: An Unprecedented Guide to the Roots, History, Strategies, and Key Documents of the Cold War*, UPA, 2015.

As far as we can see, the Putin regime, while not claiming a universal ideological solution to the world's problems as its predecessors did, nonetheless is working assiduously to gain and wield power and influence world-wide. The rise in oil prices, foreign investment, and advances in technology all fueled these efforts. More recently their economic and social position has weakened. But their continued propensity to use active measures so far has not diminished. Rather, it allows them once again to punch above their weight on the world scene and help shift the correlation of forces further in their favor without escalation to major war. They can do so because they never abandoned their playbook and many of their players.

### **What is to be Done**

So what is to be done by the U.S. in the short and longer-term?

I hope that this Open Hearing in the Committee will contribute to a much enhanced U.S. diagnostic and prescriptive policy effort that will further cauterize an ongoing problem and perhaps avoid its escalation in the future. While we seek to understand the specifics and implications of contemporary Russian behavior we can also begin to peer over the horizon. The attentive U.S. public and elected officials really ought not to be surprised again – strategically or tactically.

To help understand future Russian thinking and capabilities the following initiatives are offered that may assist in doing so.

1. Identifying in Real Time and Anticipating Russian Active Measures.
2. Reducing Russian Effectiveness.
3. Developing a strategic approach to countering Russian Active Measures.

#### **1. Identifying and anticipating Russian Active Measures**

We need enhanced warning of real-time Russian planning and their development of active measures capabilities. The U.S. National Counterintelligence Strategy of 2016 does call for the collection and analysis of the threats from foreign intelligence. We also need to anticipate—not predict—Russia's likely future operations. This will not always be possible but we should at least try. These “warnings,” in whole or in part, would be disseminated inside the U.S.

government, to selected allies, and some in the media and public so that there would be little surprise. The USG does this now with counterterrorism warnings.

## **2. Reducing Russian effectiveness.**

We should develop and implement techniques to reduce the damage caused by the Russian active measures apparatus. To some extent this can be done by the careful dissemination and follow up of the warnings. But there are a variety of additional techniques we can use regularly that would appear to mitigate or reduce the damage. One is exposure of Russian plans and operations before or after the Active Measures play out in the U.S. and abroad. Again, this was done in the 1980s, under the auspices of the State Department and the interagency group.

Another is to disseminate a positive narrative to refute specific Russian attempts to undermine the democratic narrative. This has worked previously through the “whole of government” approach, but it needs to be reinstated and enhanced.

**3. Developing a strategic approach to countering Russian Active Measures.** This is a policy as well as an intelligence issue. What should the U.S. expect and tolerate from Russia. Are there ‘red lines’ that should not be crossed? For example, should we tolerate Russian (and other) efforts to influence the mechanisms of our election process and its outcomes, now or in the future. As the FBI Director maintained recently,<sup>10</sup> we can expect them to be back—not necessarily using the same tactics – although past history suggests they tend to reuse successful ones.

How do we counter their techniques without escalating our national security problems? As one former practitioner-scholar put it, we have been able to learn how to do this with regard to nuclear weapons. There are “rules of the road” that both sides follow to avoid the catastrophe neither wants. Is there thought and research that needs to be devoted to active measures and new technologies, in addition to the Internet, that are already on the world stage with more to come?

---

<sup>10</sup> Comey, James B., Testimony Before the House Permanent Select Committee on Intelligence (HPSCI), Hearing, *Russian Active Measures Investigation*, March 20, 2017.

Should we confine ourselves to defensive, punitive methods such as sanctions? How do we respond to techniques such as “doxing” or stealing personal or government information and disclosing it at strategic moments such as elections or crises?

And should we be more politically assertive, for example, stepping up our support to elements of emerging liberal societies who are asking for our help to compete effectively against illiberal adversaries—through genuine education and advisory methods? <sup>11</sup>

\*\*\*

Again, thank you for initiating this opportunity to address an issue of such great public concern today and for the foreseeable future.

---

<sup>11</sup> Phillips, Rufus, “*Breathing Life into Expeditionary Diplomacy: A Missing Dimension of U.S. Security Capabilities*,” National Strategy Information Center, 2014.

## ACTIVE MEASURES

“Active Measures is a term that came into use in the 1950s to describe certain overt and covert techniques for influencing events and behavior in, and the action of, foreign countries. Active measures may entail influencing the policies of another government, undermining confidence in its leaders and institutions, disrupting relations between other nations, and discrediting and weakening governmental and non-governmental opponents. This frequently involves attempts to deceive the target (foreign governmental and non-governmental elites or mass audiences), and to distort the target’s perception of reality.

Active Measures may be conducted overtly through officially-sponsored foreign propaganda channels, diplomatic relations, and cultural diplomacy. Covert political techniques include the use of covert propaganda, oral and written disinformation, agents of influence, clandestine radios, and international front organizations. Although active measures are principally political in nature, military maneuvers and paramilitary assistance to insurgent and terrorists may also be involved.”

Extracted from Richard Shultz and Roy Godson, *Dezinformatsia: Active Measures in Soviet Strategy*, Pergamon-Brassey’s, 1984.

**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 Select Committee on Intelligence hearing:**

**“Disinformation: A Primer In Russian Active Measures And Influence Campaigns”**

**30 March 2017**

On 26 October 2015, I authored a post at the Foreign Policy Research Institute (FPRI) entitled “Russia Returns As Al Qaeda And The Islamic State’s Far Enemy” noting:

*“The Russians have used social media driven information campaigns to discredit the U.S. for years. Facebook and Twitter remain littered with pro-Russian, Western looking accounts and supporting automated bots designed to undermine the credibility of the U.S. government.”<sup>1</sup>*

Just a few weeks later in November 2015, the FBI visited FPRI notifying their leadership that I had been targeted by a cyber attack. The FBI didn’t say who exactly had targeted me, but I had a good idea who it might be.

In the eighteen months prior to the above quote and in the three years leading up to today, two colleagues and I watched and tracked the rise of Russia’s social media influence operations witnessing their update of an old Soviet playbook known as Active Measures.

For me, I began watching these influence operations in January 2014 after I co-authored an article in *Foreign Affairs* entitled “The Good and The Bad of Ahrar al Sham.”<sup>2</sup> Hecklers appearing to be English-speaking Europeans and Americans trolled me for my stance on Syrian President Bashar Assad. But these social media accounts, they didn’t look right - their aggression, persistence, biographies, speech patterns and synchronization were unnatural. I wasn’t the only one who noticed this pattern. Andrew Weisburd and J.M. Berger, the two best social media analysts I’d worked with in counterterrorism, noticed similar patterns around the troll discussions of Syria, Assad, al Qaeda and the Islamic State.

---

<sup>1</sup> Clint Watts (26 October 2015) *Russia returns as al Qaeda and the Islamic State’s ‘Far Enemy’*. Foreign Policy Research Institute. Available at:

<http://www.fpri.org/2015/10/russia-returns-as-al-qaeda-and-the-islamic-states-far-enemy/>

<sup>2</sup> Michael Doran, William McCants and Clint Watts (23 January 2014) *The Good and Bad of Ahrar al-Sham*. Foreign Affairs. Available at:

<https://www.foreignaffairs.com/articles/syria/2014-01-23/good-and-bad-ahrar-al-sham>

Shortly after, in March 2014, we noticed a petition on the WhiteHouse.gov website. “Alaska Back To Russia” appeared as a public campaign to give America’s largest state back to the nation from which it was purchased.<sup>3</sup> Satirical or nonsensical petitions appearing on the White House website are not out of the norm. This petition was different though, having gained more than 39,000 online signatures in a short time period. Our examination of those signing and posting on this petition revealed an odd pattern – the accounts varied considerably from other petitions and appeared to be the work of automated bots. These bots tied in closely with other social media campaigns we had observed pushing Russian propaganda.

Through the summer and fall of 2014, we studied these pro-Russia accounts and automated bots. Hackers proliferated the networks and could be spotted amongst recent data breaches and website defacements. Closely circling them were honeypot accounts, attractive looking women or passionate political partisans, which appeared to be befriending certain audience members through social engineering. Above all, we observed hecklers, synchronized trolling accounts that would attack political targets using similar talking points and follower patterns. These accounts, some of which overtly supported the Kremlin, promoted Russian foreign policy positions targeting key English speaking audiences throughout Europe and North America. From this pattern, we realized we were observing a deliberate, well organized, well resourced, well funded, wide ranging effort commanded by only one possible adversary – Russia.

*Active Measures: Everything Old Is New Again*

Soviet Active Measures strategy and tactics have been reborn and updated for the modern Russian regime and the digital age. Today, Russia seeks to win the second Cold War through “the force of politics as opposed to the politics of force”.<sup>4</sup> As compared to the analog information wars of the first Cold War, the Internet and social media provide Russia cheap, efficient and highly effective access to foreign audiences with plausible deniability of their influence.

Russia’s new and improved online Active Measures shifted aggressively toward U.S. audiences in late 2014 and throughout 2015. They launched divisive messages on nearly any disaffected U.S. audience. Whether it be claims of the U.S. military declaring martial law during the Jade Helm exercise<sup>5</sup>, chaos amongst Black Lives matter protests<sup>6</sup>

---

<sup>3</sup> The original petition is no longer accessible on the White House website but a summary of the campaign can be found at: Soraya Sarhaddi Nelson (1 April 2014) *Not An April Fools’ Joke: Russians Petition To Get Alaska Back*. NPR. Available at: <https://www.foreignaffairs.com/articles/syria/2014-01-23/good-and-bad-ahrar-al-sham>

<sup>4</sup> U.S. Information Agency (June 1992) *Soviet Active Measures in the “Post Cold War” Era 1988-1991*. U.S. House of Representatives Committee on Appropriations. Available at: [http://intellit.muskingum.edu/russia\\_folder/pcw\\_era/exec\\_sum.htm](http://intellit.muskingum.edu/russia_folder/pcw_era/exec_sum.htm)

<sup>5</sup> Dan Lamothe (14 September 2015) *Remember Jade Helm 15, the controversial military exercise? It’s over*. Washington Post. Available at:

or tensions in the Bundy Ranch standoff in Oregon<sup>7</sup>, Russia's state sponsored outlets of RT and Sputnik News, characterized as "white" influence efforts in information warfare, churned out manipulated truths, false news stories and conspiracies. Four general themes outlined these propaganda messages:

- Political Messages – Designed to tarnish democratic leaders and undermine democratic institutions
- Financial Propaganda – Created to weaken confidence in financial markets, capitalist economies and Western companies
- Social Unrest – Crafted to amplify divisions amongst democratic populaces to undermine citizen trust and the fabric of society
- Global Calamity – Pushed to incite fear of global demise such as nuclear war or catastrophic climate change

From these overt Russian propaganda outlets, a wide range of English language conspiratorial websites ("gray" outlets), some of which mysteriously operate from Eastern Europe and are curiously led by pro-Russian editors of unknown financing, sensationalize conspiracies and fake news published by white outlets further amplifying their reach in American audiences. American looking social media accounts, the hecklers, honeypots and hackers described above, working alongside automated bots further amplify and disseminate Russian propaganda amongst unwitting Westerners. These covert, "black" operations influence target audience opinions with regards to Russia and undermine confidence in Western elected leaders, public officials, mainstream media personalities, academic experts and democracy itself.

Through the end of 2015 and start of 2016, the Russian influence system outlined above began pushing themes and messages seeking to influence the outcome of the U.S. Presidential election. Russia's overt media outlets and covert trolls sought to sideline opponents on both sides of the political spectrum with adversarial views toward the Kremlin. The final months leading up to the election have been the predominate focus of Russian influence discussions to date. However, Russian Active Measures were in full swing during both the Republican and Democratic primary season and may have helped sink the hopes of candidates more hostile to Russian interests long before the field narrowed.

The final piece of Russia's modern Active Measures surfaced in the summer of 2016 as hacked materials from previous months were strategically leaked. On 22 July 2016, Wikileaks released troves of stolen communications from the Democratic National

---

[https://www.washingtonpost.com/news/checkpoint/wp/2015/09/14/remember-jade-helm-15-the-controversial-military-exercise-its-over/?utm\\_term=.10e43e79bbc8](https://www.washingtonpost.com/news/checkpoint/wp/2015/09/14/remember-jade-helm-15-the-controversial-military-exercise-its-over/?utm_term=.10e43e79bbc8)

<sup>6</sup> (2 October 2016) *Tensions at rival White & Black Lives Matter protests flare in Houston*. RT. Available at: <https://www.rt.com/usa/361346-blm-wlm-protests-houston/>

<sup>7</sup> (20 December 2016) *Hands up or charging? Conflicting reports on shooting of Oregon militia spokesman*. RT. Available at: <https://www.rt.com/usa/330365-oregon-lavoy-shooting-police/>

Committee and later batches of campaign emails. Guccifer 2.0 and DC Leaks revealed hacked information from a host of former U.S. government officials throughout July and August 2016. For the remainder of the campaign season, this compromising material powered the influence system Russia successfully constructed in the previous two years.

On the evening of 30 July 2016, my colleagues and I watched as RT and Sputnik News simultaneously launched false stories of the U.S. airbase at Incirlik being overrun by terrorists. Within minutes, pro-Russian social media aggregators and automated bots amplified this false news story and expanded conspiracies asserting American nuclear missiles at the base would be lost to extremists. More than 4,000 tweets in the first 78 minutes after launching of this false story linked back to the Active Measures accounts we'd tracked in the previous two years. These previously identified accounts, almost simultaneously appearing from different geographic locations and communities, amplified this fake news story in unison. The hashtags incrementally pushed by these automated accounts were #Nuclear, #Media, #Trump and #Benghazi. The most common words found in English speaking Twitter user profiles were: God, Military, Trump, Family, Country, Conservative, Christian, America, and Constitution. These accounts and their messages clearly sought to convince Americans a U.S. military base was being overrun in a terrorist attack like the 2012 assault on a U.S. installation in Benghazi, Libya.<sup>8</sup> In reality, a small protest gathered outside the Incirlik gate and the increased security at the airbase sought to secure the arrival of the U.S. Chairman of the Joint Chiefs of Staff the following day.<sup>9</sup>

This pattern of Russian falsehoods and social media manipulation of the American electorate continued through Election Day and persists today. Many of the accounts we watched push the false Incirlik story in July now focus their efforts on shaping the upcoming European elections, promoting fears of immigration or false claims of refugee criminality. They've not forgotten about the United States either. This past week, we observed social media campaigns targeting Speaker of the House Paul Ryan hoping to foment further unrest amongst U.S. democratic institutions, their leaders and their constituents.

As we noted two days before the Presidential election in our article describing Russian influence operations, Russia certainly seeks to promote Western candidates sympathetic to their worldview and foreign policy objectives. But winning a single election is not

---

<sup>8</sup> Andrew Weisburd and Clint Watts (6 August 2016) *How Russia Dominates Your Twitter Feed to Promote Lies*. The Daily Beast. Available at: <http://www.thedailybeast.com/articles/2016/08/06/how-russia-dominates-your-twitter-feed-to-promote-lies-and-trump-too.html>

<sup>9</sup> (1 August 2016) *Chairman in Turkey to Meet With U.S. Troops, Turkish Officials*. U.S. Department of Defense. Available at: <https://www.defense.gov/News/Article/Article/881458/chairman-in-turkey-to-meet-with-us-troops-turkish-officials>

their end goal.<sup>10</sup> Russian Active Measures hope to topple democracies through the pursuit of five complementary objectives:

- Undermine citizen confidence in democratic governance
- Foment and exacerbate divisive political fractures
- Erode trust between citizens and elected officials and democratic institutions
- Popularize Russian policy agendas within foreign populations
- Create general distrust or confusion over information sources by blurring the lines between fact and fiction

From these objectives, the Kremlin can crumble democracies from the inside out creating political divisions resulting in two key milestones: 1) the dissolution of the European Union and 2) the break up of the North American Treaty Organization (NATO). Achieving these two victories against the West will allow Russia to reassert its power globally and pursue its foreign policy objectives bilaterally through military, diplomatic and economic aggression. Russia's undeterred annexation of Crimea, conflict in Ukraine and military deployment in Syria provide recent examples.

*Why did Soviet Active Measures fail during the Cold War but succeed for Russia today?*

Russia's Active Measures today work far better than that of their Soviet forefathers. During the Cold War, the KGB had to infiltrate the West, recruit agents and promote communist parties and their propaganda while under watch by Western counterintelligence efforts. Should they be too aggressive, Soviet spies conducting Active Measures amongst U.S. domestic groups could potentially trigger armed conflict or would be detained and deported.

Social media provides Russia's new Active Measures access to U.S. audiences without setting foot in the country, and the Kremlin smartly uses these platforms in seven ways to win Western elections. First, Russia chooses close democratic contests where a slight nudge can usher in their preferred candidate or desired outcome. Second, Russia targets specific audiences inside electorates amenable to their messages and resulting influence – in particular alt-right audiences incensed over immigration, refugees and economic hardship. Third, Russia plans and implements their strategy long before an election allowing sufficient time for cultivating an amenable audience ripe for manipulation. Fourth, their early entry into electoral debates allows them to test many messages and then reinforce those messages that resonate and bring about a measurable, preferred shift in public opinion. Fifth, Russia brilliantly uses hacking to compromise adversaries and power their influence messaging – a tactic most countries would not take. Sixth, their employment of social media automation saturates their intended audience with narratives

---

<sup>10</sup> 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/>

that drown out opposing viewpoints. Finally, Russia plays either side should the contest change – backing an individual candidate or party so long as they support a Kremlin policy position and then turning against the same party should their position shift against Russia.<sup>11</sup>

The implications of Russia's new Active Measures model will be two fold. The first is what the world is witnessing today – a Russian challenge to democracies throughout the West. Russian influence surfaced in Eastern Europe elections and the United Kingdom's Brexit vote before the U.S. Presidential election, helped bolster a losing far-right candidate recently in the Netherlands<sup>12</sup> and right now works diligently to shape the upcoming 2017 elections in France and Germany. Over the horizon, Russia has provided any authoritarian dictator or predatory elite equipped with hackers and disrespectful of civil liberties a playbook to dismantle their enemies through information warfare. Fledgling democracies and countries rife with ethnic and social divisions will be particularly vulnerable to larger authoritarian regimes with the time, resources and patience to foment chaos in smaller republics.

#### *The U.S. Can Counter Russia's Modern Active Measures*

America can defuse Russia's Active Measures online by undertaking a coordinated and broad range of actions across the U.S. government. Currently, the U.S. ignores, to its own detriment, falsehoods and manipulated truths generated and promoted by Russia's state sponsored media and their associated conspiratorial websites. While many Active Measures claims seem ridiculous, a non-response by the U.S. government introduces doubt and fuels social media conspiracies. The U.S. should generate immediate public refutations to false Russian claims by creating two official government webpages acting as a U.S. government "Snopes" for disarming falsehoods. The U.S. State Department would host a website responding to false claims regarding U.S. policy and operations outside U.S. borders. The U.S. Department of Homeland Security would host a parallel website responding to any and all false claims regarding U.S. policy and operations domestically – a particularly important function in times of emergency where Russian Active Measures have been observed inciting panic.

Criminal investigations bringing hackers to justice will continue to be vital. However, the FBI must take a more proactive role during investigations to analyze what information has been stolen by Russia and then help officials publicly disclose the breach in short order. Anticipating rather than reacting to emerging Russian data dumps through public

---

<sup>11</sup> 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>

<sup>12</sup> Andrew Higgins (27 February 2017) *Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote*. New York Times. Available at: <https://www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html>

affairs messaging will help U.S. officials and other American targets of kompromat prepare themselves for future discrediting campaigns.

Russian propaganda sometime peddles false financial stories causing rapid shifts in American company stock prices that hurt consumer and investor confidence and open the way for predatory market manipulation and short selling. At times, U.S. business employees unwittingly engage with Russian social media hecklers and honeypots putting themselves and their companies at risk. The Departments of Treasury and Commerce should immediately undertake an education campaign for U.S. businesses to help them thwart damaging, false claims and train their employees in spotting nefarious social media operations that might compromise their information.

The Department of Homeland Security must continue to improve existing public-private partnerships and expand sharing of cyber trends and technical signatures. This information will be critical in helping citizens and companies prevent the hacking techniques propelling Russian kompromat. Finally, U.S. intelligence agencies have a large role to play in countering Russian Active Measures in the future, but my recommendations in this regard are not well suited for open discussion.

The most important actions to diffuse Russia's modern Active Measures actually come from outside the U.S. government – the private sector and civil society. Russia's social media influence campaigns achieve great success because mainstream media outlets amplify the salacious claims coming from stolen information. If forewarned by law enforcement of a Russian compromise (as noted above), the world's largest newspapers, cable news channels and social media companies could join in a pact vowing not to report on stolen information that amplified Russia's influence campaigns. While they would stand to lose audience in the near term to fringe outlets, Russia's Active Measures would be far less effective at discrediting their adversaries and shaping politics if they lacked access to mainstream media outlets. Mainstream media outlets unifying and choosing not to be Kremlin pawns would also be a counter to Russia's suppression of free speech and harsh treatment of journalists and the press.

Social media companies have played an outsized role in recent elections as they increasingly act as the primary news provider for their users. Tailored news feeds from social media platforms have created information bubbles where voters see only stories and opinions suiting their preferences and biases – ripe conditions for Russian disinformation campaigns.<sup>13</sup> In the lead up to the 2016 election, fake news stories were consumed at higher rates than true stories.<sup>14</sup> As a result, Facebook initiated a noble effort

---

<sup>13</sup> Yochai Benkler, Robert Faris, Hal Roberts and Ethan Zuckerman (3 March 2017) Study: Breitbart right-wing media ecosystem altered broader media agenda. Columbia Journalism Review. Available at: <http://www.cjr.org/analysis/breitbart-media-trump-harvard-study.php>

<sup>14</sup> Craig Silverman (18 November 2016) *This Analysis Shows How Viral Fake Election Stories Outperformed Real News On Facebook*. BuzzFeed. Available at:

to tag fake news stories for their readers.<sup>15</sup> But Facebook's push must be expanded and joined by other social media companies or they will be overwhelmed by the volume of stories needing evaluation and will find difficulty protecting freedom of speech and the freedom of the press.

Social media companies should band together in the creation of an Information Consumer Reports. This non-governmental agency would evaluate all media organizations, mainstream and otherwise, across a range of variables producing news ratings representative of the outlet's accuracy and orientation. The score would appear next to each outlet's content in web searches and social media streams providing the equivalent of a nutrition label for information. Consumers would not be restricted from viewing fake news outlets and their erroneous information, but would know the risks of their consumption. The rating, over time, would reduce consumption of Russian disinformation specifically and misinformation collectively, while also placing a check on mainstream media outlets that have all too often regurgitated false stories.<sup>16</sup>

Over the past three years, Russia has implemented and run the most effective and efficient influence campaign in world history.<sup>17</sup> Russian propaganda and social media manipulation has not stopped since the election in November and continues fomenting chaos amongst the American populace. American allies in Europe today suffer from an onslaught of hacks and manipulation, which threaten alliances that brought U.S. victory in the Cold War. The U.S., in failing to respond to Russia's Active Measures, will surrender its position as the world's leader, forgo its role as chief promoter and defender of democracy, and give up on over seventy years of collective action to preserve freedom and civil liberties around the world.

Our nation's democratic principles and ideals are under attack by a kleptocratic Russian regime sowing divisions amongst the American public and Western society through information warfare. Russia's strategic motto is "divided we stand, divided we fall". It's time the United States remind the world, that despite our day-to-day policy debates and political squabbles, we stand united, alongside our allies, in defending our democratic

---

[https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm\\_term=.etYEzgQno#.im3kXQAKR](https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.etYEzgQno#.im3kXQAKR)

<sup>15</sup> Olivia Solon and Julia Carrie Wong (16 December 2016) *Facebook's plan to tackle fake news raises questions over limitations*. The Guardian. Available at:

<https://www.theguardian.com/technology/2016/dec/16/facebook-fake-news-system-problems-fact-checking>

<sup>16</sup> Clint Watts and Andrew Weisburd (22 January 2017) *Can the Michelin Model Fix Fake News?* Daily Beast. Available at:

<http://www.thedailybeast.com/articles/2017/01/22/can-the-michelin-model-fix-fake-news.html>

<sup>17</sup> Kathy Frankovic (14 December 2016) *Americans and Trump part ways over Russia*. YouGov. Available at: <https://today.yougov.com/news/2016/12/14/americans-and-trump-part-ways-over-russia/>

system of government from the meddling of power-hungry tyrants and repressive authoritarians that prey on their people and suppress humanity.



**Prepared Statement of Kevin Mandia, CEO of FireEye, Inc.  
before the United States Senate Select Committee on Intelligence**

**March 30, 2017**

Thank you, Mr. Chairman, Vice-Chairman Warner, and Members of the Senate Intelligence Committee, for the opportunity you have given me today to share our observations and our experiences regarding this important topic, as well as for your leadership on cybersecurity issues. As requested, I am going to discuss three topics here today: 1) the role of overt and covert cyber operations in support of Russian active measures, disinformation, and influence campaigns; 2) the cyber capabilities and techniques attributed to Russian state and non-state actors; and 3) recommendations to prevent and mitigate the threat posed by such cyber operations.

**1. Background.**

Before I turn to your specific questions, let me share some background on myself and my company to inform the context of my narrative. I have been working in cybersecurity for over two decades, since I was first stationed at the Pentagon at the outset of my career as a Computer Security Officer in 1993. During my time investigating computer intrusions while I was in the Air Force, I came to recognize that the biggest cyber threats to our infrastructure were intrusions from other countries, most notably Russia and China. I founded Mandiant in 2004 to create a company with that could effectively respond to these threats and innovate technologies to help detect and respond to advanced attacks. Fast forward a few years, Mandiant was bought by FireEye, and I became FireEye's CEO last June in 2016.

As I testify today, FireEye employees are on the front lines of the cyber battle, responding to active computer intrusions at dozens of the largest companies and organizations on a global scale, including incidents in cyber "hot zones" such as the Middle East and Southeast Asia. Over the last 13 years, we have responded to incidents at hundreds of companies around the world. During that time, we have investigated millions of systems, and we receive calls almost every single day from organizations that have suffered a cybersecurity breach.

In addition to the 300-plus security professionals responding to computer intrusions, FireEye has over 150 cyber-threat analysts on staff in 19 countries and speaking 32 different languages, to help us predict threats and better understand the adversary – often by considering the political and cultural environment of the threat actors. We have an enormous catalog of threat intelligence, and it continues to grow everyday coincident with the continually increasing attacks on organizations around the world.



The information I will share today, then, is derived from our experiences responding to computer security breaches, as well as intelligence derived from our experienced team of cyber threat analysts and collected from more than 5000 customers who use our products to detect intrusions into their networks and respond to these attacks.

## **2. The Role of Overt and Covert Cyber Operations in Support of Russian Active Measures, Disinformation, and Influence Campaigns.**

The role of nation-state actors in cyber attacks was perhaps most widely revealed in February 2013 when Mandiant released the report, "APT1: Exposing One of China's Cyber Espionage Units," which detailed a professional cyber espionage group based in China.<sup>1</sup> Several months later in 2014 we released another report, this time regarding Russian cyber activities, entitled, "APT28: A Window into Russia's Cyber Espionage Operations?"<sup>2</sup> In that report, FireEye identified APT28 as a suspected Russian government-sponsored espionage actor, basing our conclusion on forensic details left in the malware employed since at least 2007. Since release of the initial report on APT28, we have continued to gather intelligence and collect data on the group's activities, and most recently, in January of this year, released "APT28: At the Center of the Storm"<sup>3</sup> which provides additional detail on the continued evolution of Russian cyber operations.

As shown in our most recent report, an analysis of the activities of APT28 indicates the group's interest in foreign governments and militaries, particularly those of Europe, as well as regional security organizations. In addition, our research indicates that APT28 network activity has likely supported information operations designed to influence the domestic politics of foreign nations. We provide an extensive listing of targets including the World Anti-Doping Agency (WADA), the U.S. Democratic National Committee, Mr. John Podesta, the U.S. Democratic Congressional Campaign Committee (DCCC), as well as TV5Monde and the Ukrainian Central Election Commission (CEC).

All of these breaches involved the theft of internal data – mostly emails – that was later strategically leaked through multiple forums and propagated in a manner almost certainly intended to advance particular Russian Government goals. We noted that the combination of network compromises and subsequent data leaks align closely with the Russian military's publicly stated intentions and capabilities. Russian strategic doctrine has for a long time included what the West terms 'information

---

<sup>1</sup> <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>.

<sup>2</sup> <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf>.

<sup>3</sup> <https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf>.



operations' which have been further developed, deployed and modernized. The recent activity in the United States is one of many instances of such operations conducted in support of Russian political objectives. I note that our conclusions were consistent with the U.S. Office of the Director of National Intelligence report released on January 7, 2017 in which this activity is described as "an influence campaign."<sup>4</sup>

### **3. Cyber Capabilities and Techniques Attributed to Russian State and Non-State Actors**

So how was this done, and why do we assess that the Russian government was likely behind this activity? *Let me first speak to the methodologies used.* During the course of our APT28 investigations, we analyzed over 550 customer malware variants, identified approximately 500 domains, over 70 lure documents and dozens of spear phishing emails to help us understand their tools, techniques, and procedures. We find that APT28 continues to evolve its toolkit and refine its tactics in an effort to maintain its operational effectiveness in the face of heightened public exposure and scrutiny. In addition to the continued evolution of the group's first-stage tools, we have also noted that APT28 is:

- 1 - Leveraging at least five zero-day vulnerabilities in Adobe Flash Player, Java, and Windows in 2015 alone, including CVE-2015-1701, CVE-2015-2424, CVE-2015-2590, CVE-2015-3043, CVE-2016-7193, and CVE-2015-7645.
- 2 - Increasing its reliance on public code depositories, such as Carberp, PowerShell Empire, P.A.S. webshell, Metasploit modules, and others in a likely effort to accelerate their development cycle and provide plausible deniability.
- 3 - Obtaining credentials through fabricated Google App authorization and OAuth access requests that allow the group to bypass two-factor authentication (2FA) and other security measures, and
- 4 - Moving laterally through a network relying only on legitimate tools that already exist within victims' systems, at times forgoing their traditional toolset for the duration of the compromise.

Over the past two years we have witnessed an escalation of APT 28's overall activities and one notable change in its rules of engagement. Specifically, since 2014 we have seen APT28 in many instances compromise a victim organization, steal information, and subsequently leak the stolen data into the public. Many of these leaks have been conducted through the use of "false hacktivist personas", including, among others, "CyberCaliphate", "Guccifer 2.0", "DC Leaks", "Anonymous Poland", and "Fancy Bears' Hack Team". These "personas" appropriated pre-existing hacktivist or political brands likely to obfuscate their true identity, provide plausible deniability, and to create the perception of credibility.

---

<sup>4</sup> [https://www.intelligence.senate.gov/sites/default/files/documents/ICA\\_2017\\_01.pdf](https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf).



Although we can link the collection activity to APT28, we have not been able to establish whether the APT28 operators themselves directly control the false personas that then leak material or if that responsibility instead resides with a separate entity. However, we do see similar patterns in infrastructure procurement between APT28 and some personas to suggest they played at least some role. For example, we believe that the actors behind the DCLeaks persona attempted to register the domain "electionleaks.com" one-week prior to "DCLeaks.com" in April 2016 – approximately two months prior to the first election-related leaks. These domains were registered using the service provider we have seen APT28 frequently use in the past to support cyber attacks. Thus, our intelligence indicates that APT28 likely operated with the knowledge that the data they stole during cyber intrusions would leverage these domains for public exposure of the data.

I include the following timeline and analysis to illustrate the use of these techniques over the last few years.

In June of 2014, Ukrainian officials revealed the investigation into the compromise of the Ukrainian Central Election Commission (CEC) internal network identified custom malware traced to APT28. During the May 2014 Ukrainian presidential election, purported pro-Russian hacktivists "CyberBerkut" conducted a series of malicious activities against the CEC, including a system compromise, data destruction, a data leak, a distributed denial-of-service (DDoS) attack, and an attempted defacement of the CEC website with fake election results.

In February of 2015, FireEye identified APT28 (CORESHELL) traffic beaconing from TV5Monde's network, revealing APT28 had compromised TV5Monde's network. In April 2015, alleged pro-ISIS hacktivist group CyberCaliphate defaced TV5Monde's websites and social media profiles and forced the company's 11 broadcast channels offline. We identified overlaps between the domain registration details of CyberCaliphate's website and APT28 infrastructure.

In July of 2016, the U.S. Democratic Congressional Campaign Committee (DCCC) announced that it was investigating an ongoing "cybersecurity incident" that the FBI believed was linked to the compromise of the DNC. House Speaker Nancy Pelosi later confirmed that the DCCC had suffered a network compromise. Investigators indicated that the actors may have gained access to DCCC systems as early as March. In August, the Guccifer 2.0 persona contacted reporters covering the U.S. House of Representative races to announce newly leaked documents from the DCCC pertaining to Democratic candidates. From August to October, Guccifer 2.0 posted several additional installments of what appear to be internal DCCC documents on its WordPress site.



Between March and October of 2016, investigators found that John Podesta, Hillary Clinton's presidential campaign chairman, was one of thousands of individuals targeted in a mass phishing scheme using shortened URLs that security researchers attributed to APT28. Throughout October and into early November, WikiLeaks published 34 batches of email correspondence stolen from Mr. Podesta's personal email account. Correspondence of other individuals targeted in the same phishing campaign, including former Secretary of State Colin Powell and Clinton campaign staffer William Rinehart, were published on the "DC Leaks" website.

In April through September, 2016, the U.S. Democratic National Committee (DNC) suffered a network compromise and a subsequent investigation found evidence of two breaches, attributed to APT28 and APT29. FireEye analyzed the malware found on DNC networks and determined that it was consistent with our previous observations of APT28 tools. In June 2016, shortly after the DNC's public announcement about the breach, the Guccifer 2.0 persona claimed responsibility for the DNC breach and leaked documents taken from the organization's network. Guccifer 2.0 continued to leak DNC documents through September of 2016.

And finally, in September of 2016, WADA confirmed that APT28 had compromised its networks and accessed athlete medical data. On Sept. 12, 2016, the "Fancy 'Bears' Hack Team" persona claimed to have compromised WADA and released athletes' medical records as "proof of American athletes taking doping."

Let me now turn to explaining ***why we assess that the Russian government was likely behind this activity.***

In order to make such an assessment, we reviewed and compared intrusion methodologies and tools, malware or authored exploits and use of shared personnel. We also examined forensic details that were left behind, such as the specific IP addresses or email addresses from spear phishing attacks, file names, MD5 hashes, timestamps, custom functions, encryption algorithms, or backdoors that may have command and control IP addresses or domain names embedded.

Targeting was also critical to our assessment. Knowing the types of organizations, individuals, or data that a threat group targets provided us with insight into the group's motivations and objectives. Gathering this type of data about a group typically requires visibility into the group's operational planning, their initial attacks or infection attempts, or into actual victim environments. We track all of the indicators and significant linkages associated with identified threat groups in a proprietary database that we have developed over many years comprised of millions of nodes and linkages between groups, and then analyze this information carefully in the context of the relevant political and cultural environment to develop our assessments.



Based on our extensive collected intelligence and analysis in this instance, we have determined that APT28's cyber operations are consistent with government sponsorship and control. Specifically, APT28 has relied upon a steady supply of sophisticated tools that would only have been available to a nation-state or state-protected contractor, pursued targets where Russian interests would be high, maintained a level of activity over several years requiring significant financial and personnel resources with no clear profit motive, and closely integrated its cyber attacks into broader propaganda efforts of benefit to a nation-state actor.

There are alternative explanations for APT28's sponsorship, however in our view these only appear plausible for explaining one incident at a time, and are not credible in the context of the totality of APT28's operations. By combining an increasingly wide range of technical intelligence, hands-on remediation of compromised systems, and an understanding of Russia's geopolitical aims based on its own public statements, our confidence in assessing Russian government sponsorship or control of APT28 has only grown since release of our initial report in 2014.

Moreover, the activities of APT28 are not consistent with any basic criminal activities to which we have responded, nor are they consistent with those perpetrated by a lone actor. The size of the infrastructure, the targeted information, the amount of malware and the totality of the sophistication, suggests a long-term, well-resourced espionage campaign in which Russia is the benefactor.

In summary, while we do not have pictures of a building, names of individuals, or a government agency to name, our assessment is supported by evidence of long-standing, focused operations that indicates a Russian government sponsor and government capability.

#### **4. Recommendations to Prevent and Mitigate the Threat Posed by Such Cyber Operations.**

Today, and into the foreseeable future, it is our view that the United States will face a motivated, technically sophisticated, and well-resourced adversary intent on accessing our private data, and potentially leaking it publicly. While many organizations are actively trying to counter these attacks, there currently exists a sizeable gap between what their safeguards can prevent and the ability of motivated attackers to circumvent those safeguards. Therefore, we will need to explore ways, both within and outside the cyber domain, to help deter these attacks.

Of course, all enterprises – private sector or government – should work to accurately assess their own risk profiles, and utilize updated technology and best practices to



protect their networks and systems. However, organizations cannot buy, hire or train their way to perfect security and we must consider effective deterrence and proportional response outside of the cyber domain as well.

While diplomacy is not often cited as a primary tool in this arena, evidence collected regarding Chinese activity appears to reinforce its potential effectiveness. We conducted a comprehensive study of 182 compromised U.S. targets by 72 Chinese cyber threat groups going back to 2013, and we saw a sharp decline in these operations after September 2015 – when President Obama and President Xi met and specifically agreed to curtail cyber operations for commercial benefit. To be sure, Chinese cyber operations for traditional espionage remain, and US companies are still targeted for the security, political, economic, and military intelligence that Beijing seeks. However, it appears that the agreement had an impact, demonstrating that diplomacy can also be a useful tool for reducing the cyber threat both countries face, coupled with the public-private sector collaboration. This experience leaves me optimistic that with the combined efforts of both governments and the private sector, diplomatic engagement with Russia and other nations to restrict harmful cyber activity would be enforceable.

In addition to Russia, North Korea and Iran have been tied to a series of escalating attacks that go back several years. We have been surprised by the audacity of the sponsoring nation and their willingness to surpass “redlines” that we previously believed were established. It is entirely reasonable to suspect that these nations are emboldened by each other’s behavior, and it is important to note that any response to the Russian cyber activities discussed today will likely be assessed by other countries.

Again, we applaud the leadership shown by this Committee to bring important issues such as those discussed today to light, and we in the private sector look forward to continuing to work with you to disseminate and support industry best practices and encourage adoption of comprehensive and effective cybersecurity programs across government and industry. I look forward to answering your questions today.

\* \* \*

**Prepared Statement of GEN (Ret) Keith B. Alexander\***  
**on**  
***Disinformation: A Primer in Russian Active Measures and Influence Campaigns***  
**before the**  
**United States Senate Select Committee on Intelligence**

**March 30, 2017**

Chairman Burr, Vice Chairman Warner, Members of the Committee: thank you for inviting me to discuss “*Disinformation: A Primer in Russian Active Measures and Influence Campaigns*” with you today, and specifically, how the ongoing revolution on how we create and communicate information, particularly in cyberspace, makes it easier for nations like Russia to undertake successful active measures campaigns, particularly in the realm of information operations, including overt and covert propaganda and disinformation efforts, in furtherance of national political goals. I would like to briefly touch on some of the things we ought do, working together, to combat such activities and to protect our nation—our government, our private sector, and our people—from these and other threats in cyberspace. In particular, I believe it is critical that our public and private sectors work more closely together. This Committee and the relevant agencies in the Executive Branch can play a key role in helping make that happen.

I want to thank both Chairman Burr and Vice Chairman Warner for your bipartisanship and for making cybersecurity and counterintelligence top priorities for this committee, including the Chairman’s work on the Cybersecurity Information Sharing Act and Vice Chairman Warner’s efforts with Senate Cybersecurity Caucus and on the Digital Security Commission Act. It is also worth noting that this committee has held more than 10 hearings and briefings over the last two years to examine the scale and scope of Russian activities,<sup>1</sup> and that as early as June 2016, this committee sought to require the establishment of a committee “[t]o counter active measures by Russia to exert covert influence over peoples and governments.”<sup>2</sup>

Active measures have been utilized by Russia since the 1920s, perhaps most famously during the Cold War. Retired KGB Maj. Gen. Oleg Kalugin describes these “subversion” activities as “the heart and soul of the Soviet intelligence” that were specifically designed to “weaken the West, to drive wedges in the Western community alliances of all sorts, particularly

---

\* Gen. (ret.) Keith B. Alexander is the former Director, National Security Agency and the Founding Commander, United States Cyber Command. Currently, he is the President and CEO of IronNet Cybersecurity and recently completed service as a member of the President’s Commission on Enhancing National Cybersecurity.

<sup>1</sup> See Federal News Service, *Transcript: Full Committee Hearing on Russian Intelligence Activities*, Senate Select Committee on Intelligence (Jan. 10, 2017).

<sup>2</sup> See Intelligence Authorization Act for Fiscal Year 2017 § 501, *available online at* <<https://www.intelligence.senate.gov/legislation/intelligence-authorization-act-fiscal-year-2017-reported-june-6-2016>>.

NATO, [and] to sow discord among allies.”<sup>3</sup> According to Kalugin, this “worldwide campaign...conducted and manipulated by the KGB,” included “all sorts of forgeries and faked material...targeted at politicians, the academic community, [and the] public at large.”<sup>4</sup> Likewise, Vasili Mitrokhin, a former senior KGB archivist, described the bulk of KGB active measures as “‘influence operations’ designed to discredit the [United States]...[through] disinformation fabricated by...the active measures branch of the [KGB].”<sup>5</sup> During the Cold War, these activities included efforts to undermine the FBI, the State Department, and civil rights leaders, as well as efforts to incite racial violence and hatred, including through the dissemination of false information about private organizations, individuals, and the government via false publications and materials misattributed to particular individuals or organizations, among other things.<sup>6</sup>

In many ways, this description of historic Soviet active measures is strikingly similar to what this committee described last year as Russian covert influence active measures, including the “[e]stablishment or funding of [ ] front group[s]...[c]overt broadcasting...[m]edia manipulation...[and] [d]isinformation and forgeries, funding agents of influence, incitement, and offensive counterintelligence, assassinations, or terrorist acts.”<sup>7</sup> Director Clapper likewise indicated that “Moscow’s influence campaign blended covert intelligence operations with overt efforts by Russian government agencies, state funded media, third party intermediaries and paid social media users” and that “Moscow’s behavior reflects Russia’s more aggressive cyber posture in recent years, which poses a major threat to U.S. military, diplomatic, commercial and critical infrastructure networks. ...[and] demonstrate[s] a significant escalation in directness, level of activity, and scope of effort compared to previous operations.”<sup>8</sup>

At the same time, it is certainly worth noting that aggressive efforts to collect intelligence on our elections are not new – indeed, ODNI has made clear that in 2008, the “foreign intelligence services...track[ed the] election cycle like no other” and “targeted the campaigns...[m]et with campaign contacts and staff[,] [u]sed human source networks for policy insights, [e]xploited technology to get otherwise sensitive data, [and] [e]ngaged in perception management to influence policy.”<sup>9</sup> Indeed, Russia use of *komprodat* (compromising information), *maskirovka* (military deception), and proxy assets to disseminate propaganda (both official and unofficial) is likewise not new.

---

<sup>3</sup> See CNN, *Inside the KGB: An Interview with Maj. Gen. Oleg Kalugin* (Jan. 1998), available online at <<https://web.archive.org/web/20070206020316/http://www.cnn.com/SPECIALS/cold.war/episodes/21/interviews/ka-lugin/>>.

<sup>4</sup> *Id.*

<sup>5</sup> *Id.*

<sup>6</sup> See, e.g., *id.* at 234-39.

<sup>7</sup> See Intelligence Authorization Act for Fiscal Year 2017 § 501.

<sup>8</sup> *Id.*

<sup>9</sup> See ODNI, *Unlocking the Secrets: How to Use the Intelligence Community* (Dec. 10, 2008), at 12-13, available online at <<https://icontherecord.tumblr.com/post/143906537893/new-freedom-of-information-act-request-documents>>.

Efforts like these are empowered by the modern era of technology and, in particular, by the scale and scope of information traversing our networks. The amount of information circulating the globe via IP networks will reach 2.3 zettabytes by 2020, the “equivalent of all the movies ever made [] cross[ing] the global Internet every 2 minutes.”<sup>10</sup> And it will be transmitted over 26.3 billion networked devices, more than three IP-connected devices per person worldwide.<sup>11</sup> At the same time, according to Pew Research, “a majority of U.S. adults – 62% – get news on social media,” and given the penetration of some of these services, message targeting can be broad in scale yet highly focused. For example, Pew estimates up to 44% of the general population in the United States gets some measure of its news on Facebook.<sup>12</sup> And given the continued development and rapid iteration of technology and Internet-enabled platforms, these trends are likely to continue and even accelerate.

While this might not seem particularly troubling at first blush, it is worth evaluating in the context of potential efforts to manipulate information. Back in the Cold War era, if the Soviet Union sought to manipulate information flow, it would have to do so principally through its own propaganda outlets or through active measures that would generate specific news: planting of leaflets, inciting of violence, creation of other false materials and narratives. But the news itself was hard to manipulate because it would have required actual control of the organs of media, which took long-term efforts to penetrate. Today, however, because the clear majority of the information on social media sites is uncurated and there is a rapid proliferation of information sources and as other sites that can reinforce information, there is an increasing likelihood that the information available to average consumers may be inaccurate (whether intentionally or otherwise) and may be more easily manipulable than in prior eras. It is likewise easier to generate “buzz” and “hype” about particular events or storylines (again, whether accurate or inaccurate) because of the speed at which news is conveyed amongst the population.

These efforts also take place in the context of larger cyber efforts by our peer competitors, including the ongoing, massive theft of intellectual property from American companies and the use of actual destructive attacks on both public and private sector entities in the United States and abroad.<sup>13</sup> The reality is that as a free society, we have many vulnerabilities and leave ourselves open to threats—including propaganda and disinformation attacks—that more authoritarian nations may be more capable of combatting by limiting access to resources or restricting the freedom of their people. And it is worth noting that our enemies today need not attack our government to have a substantive strategic effect on our nation. Attacking civilian or

---

<sup>10</sup> See Cisco, *The Zettabyte Era—Trends and Analysis* (June 2016) at 1, 4, available online at <<http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.pdf>>

<sup>11</sup> See *Zettabyte Era*, n. 3 *supra* at 2.

<sup>12</sup> *Id.*

<sup>13</sup> These activities include destructive attacks against Saudi Aramco and Qatari RasGas in 2012, more recent attacks against the Saudi government, and destructive attacks conducted by nation-states against private institutions in the United States, including the Las Vegas Sands Corporation and Sony Corporation, not to mention massive disruptive attacks targeting American financial institutions. See Keith B. Alexander, *Prepared Statement on A Borderless Battle: Defending Against Cyber Threats*, U.S. House Committee on Homeland Security (March 22, 2017), at 2 & n. 1-3, available online at <<http://docs.house.gov/meetings/HM/HM00/20170322/105741/HHRG-115-HM00-Wstate-AlexanderK-20170322.pdf>>.

economic targets, including through disinformation, may be a more effective approach in the modern era, particularly for asymmetric actors like terrorist groups. Moreover, as the number of nations that possess the capability to exploit and attack continues to grow, there is more of a chance that those with less of an incentive to act in line with appropriate state-to-state behavior will begin using cyber capabilities in a more aggressive way.

What all of this fundamentally means is that the future of warfare—including information operations—is here, and we need to structure and architect our nation to defend our country in cyberspace. Specifically, in my view, it is critical that as a nation, we fundamentally rethink how the government and the private sector relate to one another in cyberspace. We need to draw clear lines and make explicit certain responsibilities, capabilities, and authorities. And because the private sector controls the vast majority of the real estate in cyberspace, particularly when it comes to critical infrastructure and key resources,<sup>14</sup> there is no question that the government and private sector must collaborate. We need to recognize that neither the government nor the private sector can capably protect the systems and networks that our nation relies upon without extensive and close cooperation.

For the government to effectively work with the private sector to secure the nation in cyberspace, perhaps the single most important thing the government can do is to build real connectivity and interoperability with the private sector. This effort must be a two-way partnership between government and the private sector: the government can and must do more when it comes to partnering with the private sector, building trust, and sharing threat information—even highly classified threat information—at network speed, and in a form that can be actioned rapidly. Building out a cross-cutting information sharing capability allows the government and private sector to develop a common operating picture, analogous to the air traffic control picture. Just as the air traffic control picture ensures our aviation safety and synchronizes government and civil aviation, the cyber common operational picture can be used to synchronize a common cyber defense for our nation, drive decision-making, and enable rapid response across our entire national cyber infrastructure. In my view, if properly implemented, this could prove a critical defensive capability for the nation.

While much remains to be done to fully put our nation on a path to real security in cyberspace, I am strongly hopeful for our future. With your leadership, Mr. Chairman, and that of the Vice Chairman, working together collaboratively across the aisle and with the White House and key players in the private sector, as well as other key committees in Congress, I think we can achieve some real successes in the near future.

---

<sup>14</sup> See, e.g., Office of the Director of National Intelligence, Office of the Program Manager-Information Sharing Environment, *Critical Infrastructure and Key Resources*, available online at <<https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources>> (“The private sector owns and operates an estimated 85% of infrastructure and resources critical to our Nation’s physical and economic security.”).

# **DISINFORMATION**

## **A PRIMER IN RUSSIAN ACTIVE MEASURES AND INFLUENCE CAMPAIGNS**

---

---

### **HEARINGS**

BEFORE THE

## **SELECT COMMITTEE ON INTELLIGENCE**

## **UNITED STATES SENATE**

**ONE HUNDRED FIFTEENTH CONGRESS**

**30 MARCH 2017, 2PM, HART OFFICE BUILDING**

---

[INTELLIGENCE.SENATE.GOV/HEARINGS/OPEN-HEARING-INTELLIGENCE-MATTERS-1](https://intelligence.senate.gov/hearings/open-hearing-intelligence-matters-1)

Thomas Rid\*

Understanding “cyber operations” in the 21st century is impossible without first understanding intelligence operations in the 20th century. Attributing and countering disinformation operations today is therefore also impossible without first understanding how the US and its European allies attributed and countered thousands of active measures throughout the Cold War.

Active measures are semi-covert or covert intelligence operations to shape an adversary’s political decisions. Almost always active measures conceal or falsify the *source*—intelligence operators try to hide behind

---

\* Professor of Security Studies, King’s College London. @RIDT

anonymity, or behind false flags. Active measures may also spread forged, or partly forged, *content*. The most concise description of disinformation as an intelligence discipline comes from one of its uncontested grandmasters, Colonel Rolf Wagenbreth, head of the East German Stasi's Active Measures Department X for over two decades:

A powerful adversary can only be defeated through [...] a sophisticated, methodical, careful, and shrewd effort to exploit even the smallest 'cracks' between our enemies [...] and within their elites.<sup>1</sup>

The tried and tested way of active measures is to use an adversary's existing weaknesses against himself, to drive wedges into *pre-existing* cracks: the more polarized a society, the more vulnerable it is—America in 2016 was highly polarized, with myriad cracks and fissures to drive wedges into. Not old wedges, but improved high-tech wedges that allowed Moscow's operators to attack their target faster, more reactively, and at far larger scale than ever before.

Yet there was one big problem. The Russian disinformation operators also left behind more clues and traces than ever before. Thus the evidence implicating Russian intelligence in hacking-and-leaking operations over the past two years is also more granular than ever before. This digital forensic evidence can only adequately be assessed by looking at the wider picture of the 2016 influence campaign against the US election.

First: *in the past 60 years, active measures became the norm*. Russia's intelligence services pioneered *dezinformatsiya* in early twentieth century. By the mid-1960s, disinformation—or active measures—were well-resourced and nearly on a par with collection in the KGB, the Stasi's HVA, the Czechoslovak StB, and others. The Cold War saw more than 10,000 individual Soviet bloc disinformation operations.<sup>2</sup> The pace of Russian operations subsided during a short lull in the early 1970s, followed by an all-time high-water mark in the mid-1980s, and then a long intermission throughout the 1990s. Only in the late 2000s did disinformation begin to pick up speed again. By 2015 and especially 2016, the old playbook had been successfully adapted to a new technical environment.

Second, *in past 20 years, aggressive Russian digital espionage campaigns became the norm*. The first major state-on-state campaign was MOONLIGHT MAZE, which started in late 1996.<sup>3</sup> Ten years later American and European intelligence agencies and soon also an expanding number of private sector companies were tracking at least three different hacking groups linked to Russia's main intelligence agencies: tracking their implants and tools, their

infrastructure, their evolving methods of operation, their targeting behavior, their evolving operational security, and—perhaps most importantly—the mistakes the Russian operators made again and again. In 2014 a shift in tactics became apparent especially in military intelligence: a once careful, risk-averse, and stealthy espionage actor became more and more careless, risk-taking, and error-prone. One particularly revealing operational security slip-up resulted in a highly granular view of just one slice of GRU<sup>4</sup> targeting between 16 March 2015 and 17 May 2016—that slice contained 19,300 malicious links, targeting around 6,730 individuals.<sup>5</sup> A high-resolution picture of Russia’s digital espionage activities emerged.<sup>6</sup>

Third, *in past 2 years, Russian intelligence operators began to combine the two, hacking and leaking*—or digital espionage and active measures.

By early 2015, GRU was targeting military and diplomatic entities at high tempo, especially defense attachés world-wide. Among the targets are numerous senior US military officers and defense civilians, for example the private accounts of the current chairman of the Joint Chiefs of Staff, General Joseph F. Dunford; Generals Philip Breedlove, Wesley Clark, and Colin Powell; Navy Captain Carl Pistole, or current Assistant Secretary of the Air Force Daniel Ginsberg. Among the diplomatic targets were the current US ambassador to Russia, John F. Tefft; his predecessor Michael McFaul; former Permanent Representatives to NATO Ivo Daalder and Kurt Volker; and well-connected security experts Anthony Cordesman, Julianne Smith, and Harlan Ullman. The targets also included a large number of diplomatic and military officials in Ukraine, Georgia, Turkey, Saudi Arabia, Afghanistan, and many countries bordering Russia, especially their military attachés, all legitimate and predictable targets for a military intelligence agency. Russian intelligence also targeted well-known Russian critics, for example the author Masha Gessen, Garry Kasparov, and Alexei Navalny, as well as the Russia-based hacker group Shaltay Boltai. In early 2015, the same entity often referred to as APT28 or FANCYBEAR had successfully breached not just the German Parliament;<sup>7</sup> the Italian military;<sup>8</sup> but also Saudi Arabia’s foreign ministry.

Then, in May and June 2015, the first publicly known large-scale disinformation operation, dubbed “Saudi Cables,” tested an innovative tactic: hacking a target, exfiltrating compromising material (*kompromat*), setting up a dedicated leak website under false flag, and then passing files to Wikileaks for laundering and wide distribution.<sup>9</sup> Between June 2015 and November 2016, at least six front organizations sprung up as outlets

for compromised files by GRU: Yemen Cyber Army, Cyber Berkut, Guccifer 2.0, DC Leaks, Fancy Bears Hack Team, and @ANPoland.

Finally, *in past year, the timeline of US-election operations began to align*. In early March, GRU began to train its well-established, semi-automated targeting tools from worldwide military and diplomatic targets to US political targets. Between 10 March and 7 April, GRU targeted at least 109 Clinton campaign staffers with 214 individual phishing emails (with 8 more attempts on 12 and 13 May). 36 times Clinton staffers clicked a malicious link (the success rate of actually breaching the account after a victim clicked this link is 1-in-7). Russian intelligence targeted Jake Sullivan in at least 14 different attempts beginning on 19 March, each time with a different malicious link against two of his email addresses. GRU targeted Hillary Clinton's personal email account at least two times in March, but the available data show that she did not fall for the password reset trick. The military intelligence agency also targeted DNC staffers with 16 emails between 15 March and 11 April, and 3 DNC staffers were tricked into clicking the treacherous "reset password" button on 6 April 2016.

Less than two weeks later, on 19 April, the front website DCLeaks.com was registered as a leak outlet for hacked files.<sup>10</sup> The overlap between individuals hacked by GRU and leaked by "DC Leaks" aligns nearly perfectly: out of 13 named leak victims,<sup>11</sup> the available forensic evidence identifies 12 as targeted by GRU, with a spike of activity in late March 2016 (all US victims except George Soros).<sup>12</sup> The Russian-orchestrated leak operation continued apace during the hot summer of 2016 using, often with small batches of files released in more than 80 individual leaks for the best publicity effect.

The *publicly available* evidence that implicates Russian intelligence agencies in the 2016 active measures campaign is extraordinarily strong. The DNC hack can be compared to a carefully executed physical break-in in which the intruders used uniquely identical listening devices; uniquely identical envelopes to carry the stolen files past security; and uniquely identical getaway vehicles.

Listening devices (*implants*): the DNC intruders reused implants that had been deployed in a very large number of Russian intrusions across many hundreds of targets in dozens of countries over the past decade.<sup>13</sup> The implants shared many common features, among them a specific communication protocol and other modular functionality—comparable to

using the exact same listening device in different buildings without ever publishing the design plans for it.<sup>14</sup>

Getaway vehicle (*command-and-control infrastructure*): Russian intelligence agencies reused command-and-control sites—a common technique comparable to using the same getaway car with identical license plates in a burglary.<sup>15</sup> The infrastructure re-use is not easily forged, and allowed investigators to link the DNC breach to other breaches with high confidence, particularly to the German Bundestag hack, which the German government had already attributed to Russian military intelligence.

Envelopes (*encryption keys*): Russian operators also reused encryption keys across different targets, notably in targeting Ukrainian artillery units deployed against Russia-supported separatists as well as a Democratic organization in Washington, as well as in at least 75 other implants across a large number of targets world-wide.<sup>16</sup> This cryptographic overlap is an exceptionally strong forensic link, comparable to a human fingerprint.

But a narrow technical analysis would miss the main political and ethical challenges. Soviet bloc disinformation specialists perfected the art of exploiting *unwitting agents*.<sup>17</sup> In early 1980s, for example, there was no contradiction between being a genuine, honest, innocent peace activist against NATO's Double Track Decision—and at the same time being an unwitting agent for the Soviet cause. The internet has made unwitting agents more potent, more persistent, and more pervasive.

Three different types of unwitting agents stand out in the 2016 campaign. The first is Wikileaks. During the 2016 influence operation Russian intelligence agencies have abused anonymity tools for hacking<sup>18</sup>—and for leaking. Wikileaks was purpose-created to anonymize leaks. The controversial platform is a dream-come-true for active measures operators. Those Russian intelligence officers tasked with utilizing Wikileaks will likely play by their old playbook: any unwitting agent is more effective when left in the belief that they are genuinely holding the moral high-ground, not representing an authoritarian intelligence agency.

The second major unwitting agent has been Twitter, the social media platform most influential among opinion-leaders. Fully automated bots as well as semi-automated spam and trolling accounts make up a sizeable part of Twitter's active user base.<sup>19</sup> The company could easily generate statistics on how many accounts are automated bots or semi-automated to amplify disinformation or bully opponents; how many interactions and

engagements with politically influential accounts during the 2016 campaign were actual human; and likely how many of those engagements were controlled from abroad or deliberately obfuscated. But the social media firm has a commercial incentive to hide or understate these figures, as they inflate the active user numbers, a precious measure for social media companies. The result is a platform practically purpose-built for active measures: easy exploitation—high impact.

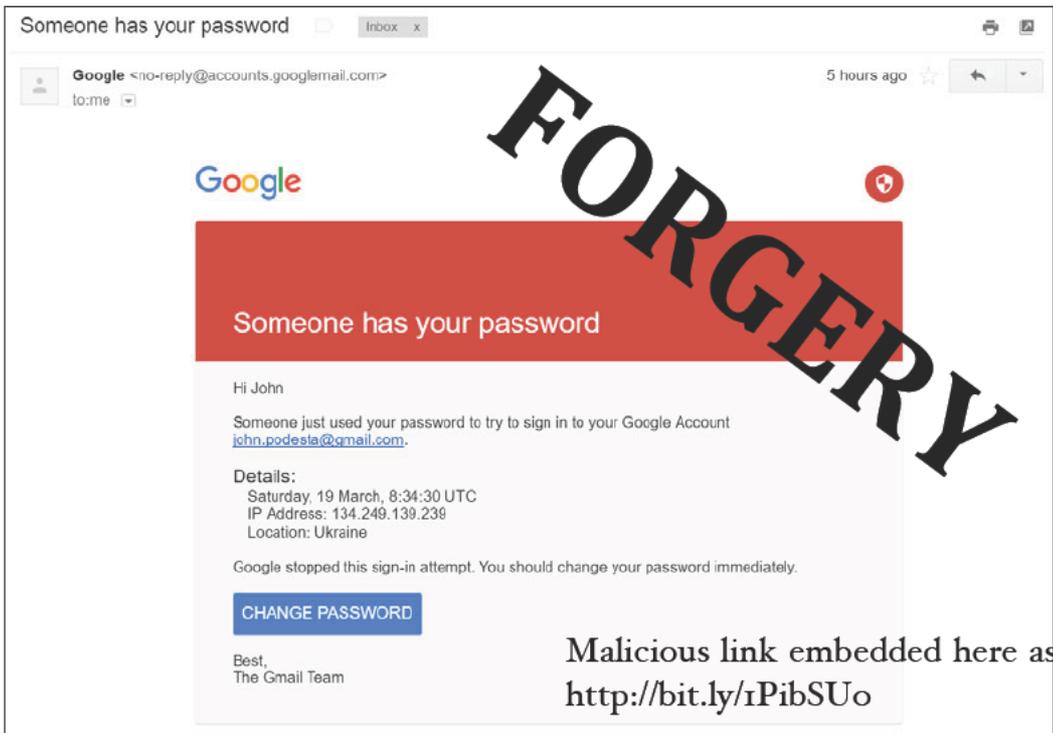
The third group of unwitting agents of 2016 were those journalists who aggressively covered the political leaks while neglecting or ignoring their provenance. Soviet bloc active measures have skillfully fed forgeries and selected documents to journalists many hundreds of times. But doing so required handiwork and craftsmanship: preparing documents; writing cover letters; trust-building; or covert and cumbersome surfacing operations. Cold War disinformation was artisanal; today it is outsourced, at least in part—outsourced to the victim itself. American journalists would dig deep into large dumps, sifting gems, mining news, boosting ops.

“Sometimes I am amazed how easy it is to play these games,” said the KGB’s grandmaster of *dezinformatsiya*, General Ivan Agayants, during an inspection of the particularly aggressive active measures shop in Prague in 1965, “if they did not have press freedom, we would have to invent it for them.”<sup>20</sup> — Three years later the operator Agayants was speaking with would defect to the US. In 1980 Ladislav Bittman testified on Russian Active Measures here in Congress. “The press should be more cautious with anonymous leaks,” Bittman told the Permanent Select Committee on Intelligence, “Anonymity is a signal indicating that the Big Russian Bear might be involved.”

**Exhibit 1**

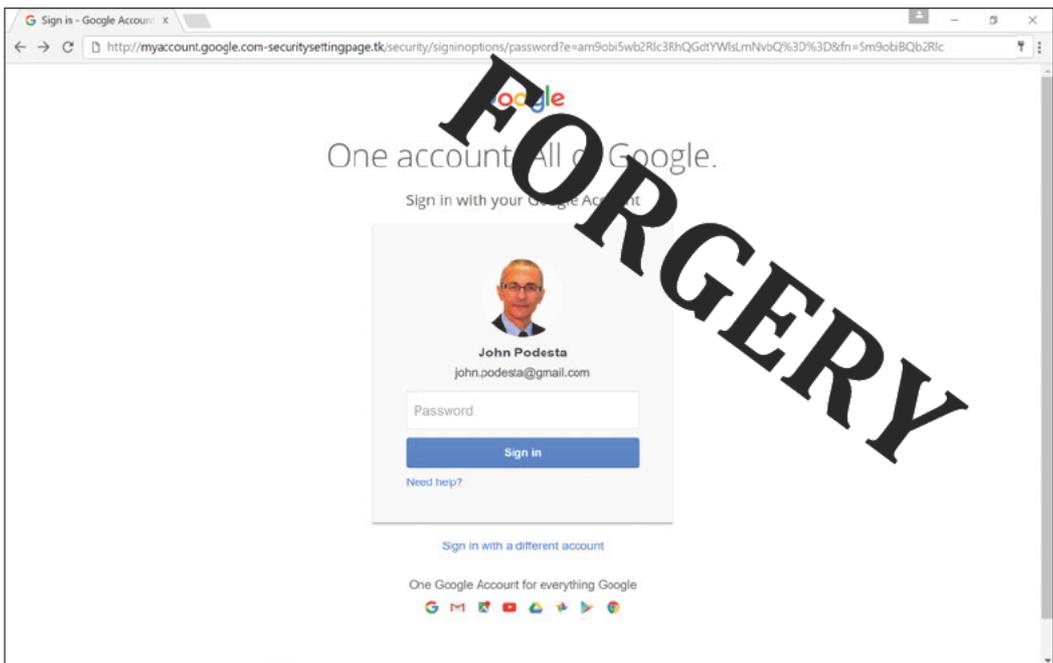
Sample GRU aka APT28/FANCYBEAR phishing email sent on 2 June 2015 (original).

### Exhibit 2

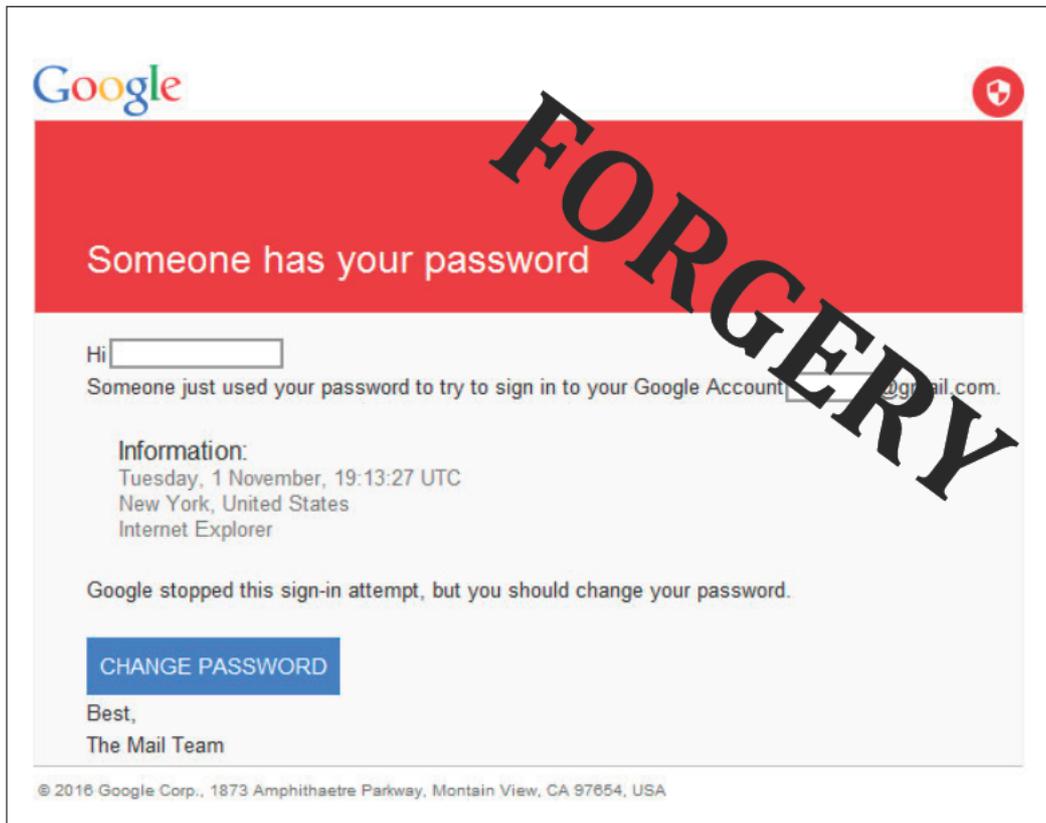


Phishing email sent to John Podesta (reconstruction by Matt Tait). Note the tradecraft: the “o”s in “someone has your password” are unicode homoglyphs, presumably to evade Google’s spam filters.

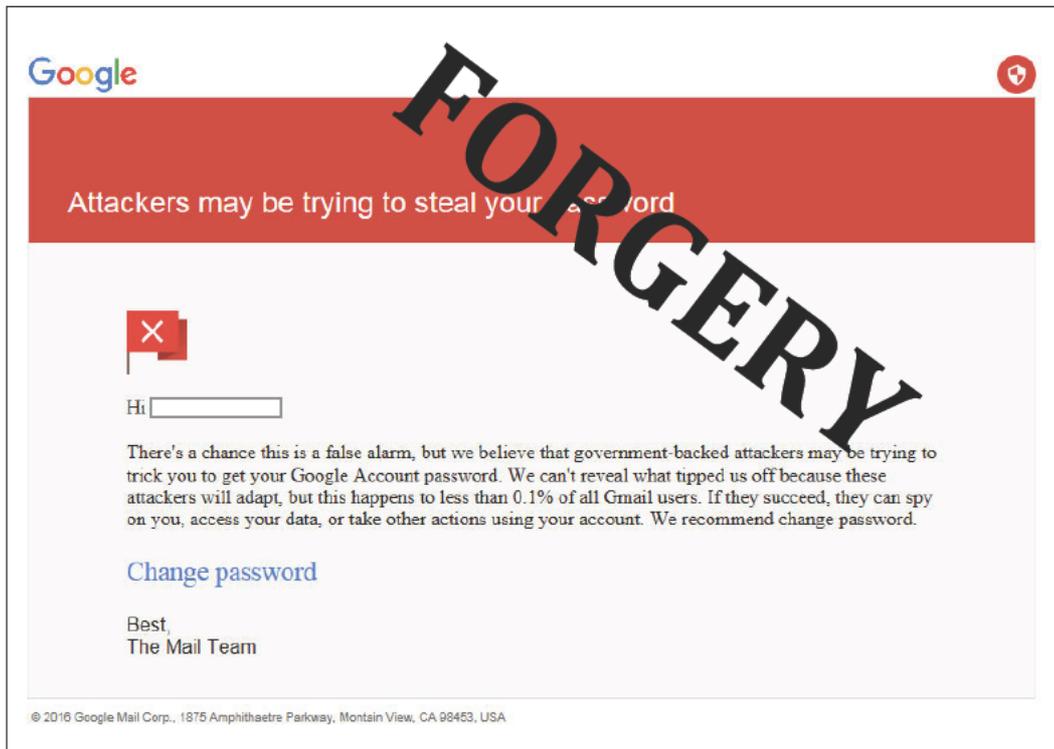
### Exhibit 3



Password credential harnessing site, prefilled with John Podesta’s picture, name, and email-address. Note the deceptive URL, with a dash, not a forward slash, after google.com, thus pointing to com-securitysettings.tk (reconstruction by Matt Tait).

**Exhibit 4**

APT28/FANCYBEAR phishing email that fairly accurately represents legitimate warnings from Google. Note the flawed spelling in the address footer. This email was in fact sent from a yandex.com address but made to appear as a Google address. It included a TinyURL-shortened link on the "CHANGE PASSWORD" button (original).

**Exhibit 5**

Here APT28/FANCYBEAR, a state-backed attacker, sent a phishing email camouflaging as a state-backed attackers warning. Notably Google's legitimate message is only displayed in the Gmail user interface and never sent via email. This email was sent from a mail.com address, and included a TinyURL-shortened link on the "Change password" link (original).

## Exhibit 6

bitly TOUR ENTERPRISE RESOURCES ABOUT MY ACCOUNT

! This link has been flagged as redirecting to malicious or spam content.

MAY 13, 2015

<http://accounts.pass-google.com/ServiceLogin?https://accounts.google.com/Service...>

<http://accounts.pass-google.com/ServiceLogin?https://accounts.google.com/ServiceLogin?passive=1209600&osid=1&continue=https://myaccount.google.com/&followup=https://myaccount.google.com/&authuser=0&continue=https://security.google.com/settings/security/activity?pii=1&rapt=JmU9YndhbmFmMTAZ21haWwuY29JmZuPVBoaWwgQnJlZWRSb3ZlJm49UGhpbCZpbWc9bitly.com/1lxj1Sw> COPY

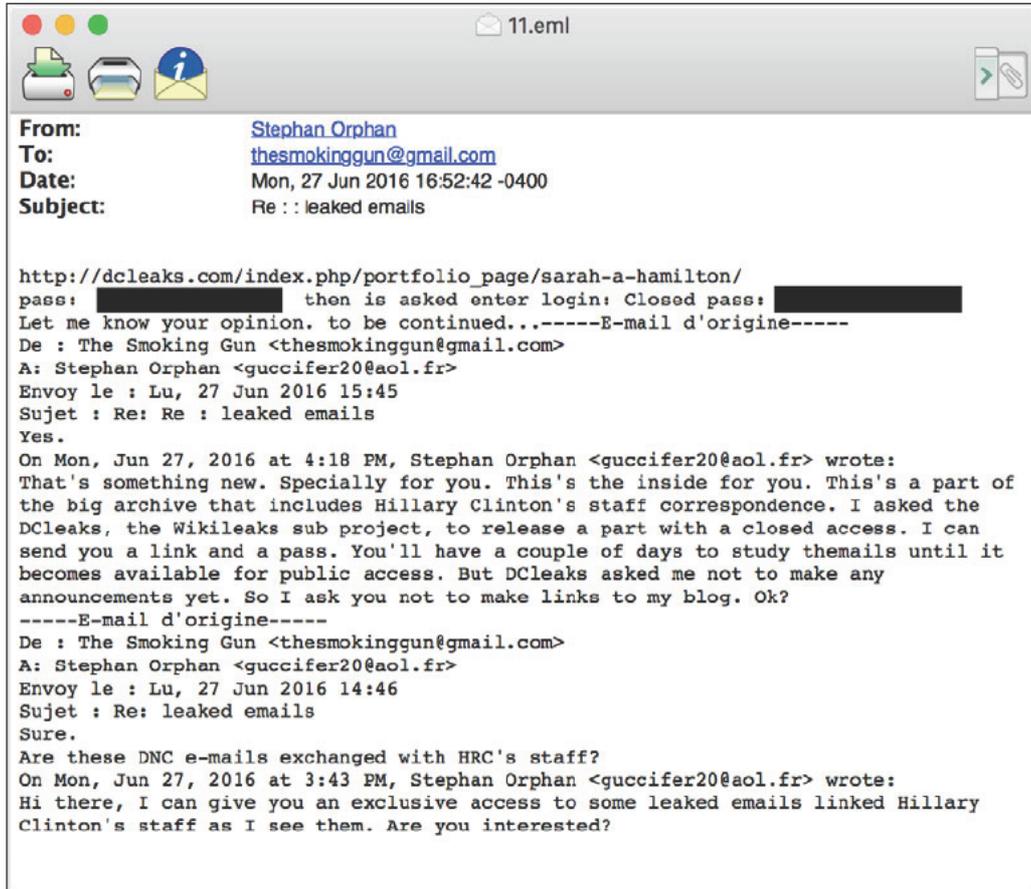
2 <sup>alpha</sup> CLICKS

Base64 decodes to: "bwanaf16@gmail.com," and Phil Breedlove

SEP '14 SEP '15 SEP '16

The Russian phishing URL with General Philip M. Breedlove's private email address and name encoded to pre-fill the forged login form. Breedlove was likely compromised in mid-May 2015, less than two weeks after ending his service as Supreme Allied Commander Europe. He became the first leak victim on DC Leaks in June 2016.

## Exhibit 7



An operational security slip-up from 27 June 2016 in which one front account, Guccifer 2.0, offers non-public access credentials (password redacted) belonging to another front account, DC Leaks, to *The Smoking Gun*. The operators thus provided another forensic artifact to link the two fronts to each other, and to the wider Russian active measures campaign of 2016. Source: "Does a BEAR Leak in the Woods?" *ThreatConnect Research Team*, Arlington, VA: ThreatConnect, 12 August 2016.

## Exhibit 8



The likely APT28/FANCYBEAR front website Wikisaleaks.com, captured on 10 August 2015, with the note that files had been provided to Wikileaks. The full-length site is depicted on the right. The captured version is at <http://web.archive.org/web/20150810005744/http://www.wikisaleaks.com/>

## Endnotes

<sup>1</sup> Günter Bohnsack, Herbert Brehmer, *Auftrag Irreführung*, Carlsen, 1992, p. 16.

<sup>2</sup> Lawrence Martin (Ladislav Bittman), in interview with Thomas Rid, 25 March 2017, Rockport, MA. See also Bittman, Ladislav, *The Deception Game*, Syracuse University Research Corporation, 1972.

<sup>3</sup> Thomas Rid, *Rise of the Machines*, New York: Norton, 2016, last chapter.

<sup>4</sup> Three of the most potent Western intelligence communities agree with the APT28/FANCYBEAR attribution to Russian military intelligence: the United States; Germany; and the United Kingdom.

<sup>5</sup> SecureWorks shared the full dataset with the author. See also "Threat Group 4127 Targets Hillary Clinton Presidential Campaign," *SecureWorks Counter Threat Unit*, 16 June 2016, as well as "Threat Group-4127 Targets Google Accounts," *SecureWorks Counter Threat Unit*, 26 June 2016.

Out of 19,315 malicious links sent, 3,134 were clicked at least once—just above 16 percent. If the password harvesting success rate is 1-in-7, then the total number of compromised accounts in this set would be around 470, which would mean an overall success rate of 2.4 percent. This estimate is conservative, as the total number of clicks is understated for technical reasons.

<sup>6</sup> The number of private sector reports on the entity codenamed APT28, FANCYBEAR, Sofacy, Sednit, Pawn Storm, STRONTIUM is in the three digits, many of them unfortunately not publicly available. One of the first public reports was *APT28: A Window into Russia's Cyber Espionage Operations?* Milpitas, CA: Fireeye, 27 October 2014.

<sup>7</sup> See “Deutsche Beamte beschuldigen russischen Militärgeheimdienst,” *Der Spiegel*, 30 January 2016. Also: “Nachrichtendienstlich gesteuerte elektronische Angriffe aus Russland,” *BfV Newsletter*, Beitrag Spionageabwehr, January 2016.

<sup>8</sup> Stefano Maccaglia, “Evolving Threats: dissection of a Cyber- Espionage attack,” Abu Dhabi: RSA Conference, November 2015.

<sup>9</sup> Brian Bartholomew and Juan Andrés Guerrero-Saade, “Wave your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks,” *Virus Bullentin Conference*, 6 October 2016. (For a more extensive analysis: “TLP Amber” report from autumn 2015 by a major security company, <https://www.us-cert.gov/tlp>). The attribution of this Saudi operation is particularly difficult. I would assess with moderate confidence that “Wikileaks” was a Russian intelligence operation and that Yemen Cyber Army was a Russian front.

<sup>10</sup> For registration information, see <http://whois.domaintools.com/dcleaks.com>

<sup>11</sup> American victims whose personal emails were subsequently leaked on DC Leaks are Philip Breedlove, Sarah Hamilton, Brian Keller, Zachary Leighton, Capricia Marshall, Ian Mellul, Beanca Nicholson, Carl Pistole, Colin Powell, Sarah Stoll, William Rinehart, and John Podesta (where GRU used Wikileaks as an outlet).

<sup>12</sup> John Podesta was targeted on 19 March; Rinehart on the 22nd; Hamilton, Leighton, Nicholson, and Mellul on the 25th.

<sup>13</sup> Google reported that “Portions of the X-Agent code base can be found in malware dating back to at least 2004,” see Neel Mehta, Billy Leonard, Shane Huntley, “Peering into the Aquarium,” Palo Alto: Google Security Team, 5 September 2014, p. 20.

<sup>14</sup> The APT28/FANCYBEAR communication protocol is a strong forensic link between breaches against Washington-based political organizations, the compromised app used against Ukraine artillery units, the German Bundestag breach, and other operations. The full source code of the so-called X-Agent implant in question was not publicly available by 27 March 2017. CrowdStrike’s Adam Myers, interview with author, Washington, DC, 27 March 2017. See Exhibit 1 for GRU’s X-Agent communication protocol.

<sup>15</sup> One example is a re-used IP address, 176.31.112[.]10, which was hardcoded into two DNC implant samples:

```
4845761c9bed0563d0aa83613311191e075a9b58861e80392914d61a21bad976, and
40ae43b7d6c413becc92b07076fa128b875c8dbb4da7c036639eccf5a9fc784f;
as well as in the Bundestag sample,
730a0e3daf0b54f065bdd2ca427f1e0e8d4e28646a5dc40cbcfb15e1702ed9a.
```

<sup>16</sup> The 50-bytes RC4 keys had a 46-bytes overlap. The keys were hardcoded into the X-Agent implants that were deployed against the Linux server of a Washington-based political organization—and against Android devices of Ukrainian artillery units in Eastern Ukraine. A member of the 55th Artillery Brigade developed a legitimate targeting app, named Понп-Д30.apk, in early 2013. By late April 2013 a rigged version of that app was offered for download on social media platforms used by the artillery units; this compromised app contained the implant with the similar RC4 key. Below the Linux 50-bytes key, followed by the Android key, with 46 bytes overlap (non-overlapping bytes in square brackets):

```
3B C6 73 0F 8B 07 85 C0 74 02 FF [D0 83] C7 04 3B FE 72 F1 5F 5E C3 8B FF 56 B8 D8 78 75
07 50 E8 B1 D1 [FF FF] 59 5D C3 8B FF 55 8B EC 83 EC 10 A1 33 35
```

```
3B C6 73 0F 8B 07 85 C0 74 02 FF [CC DE] C7 04 3B FE 72 F1 5F 5E C3 8B FF 56 B8 D8 78 75
07 50 E8 B1 D1 [FA FE] 59 5D C3 8B FF 55 8B EC 83 EC 10 A1 33 35
```

The RC4 keys strongly link at least 76 different samples in the CrowdStrike’s intelligence library, all positively attributed to APT28/FANCYBEAR implants or loaders, aka GRU. The Ukrainian military’s Android app may have been operationally less effective than initially portrayed. But

the effectiveness of the app is an issue entirely unrelated to the targeting itself. The forensic significance of quality artifacts found in the implants is strong, especially the cryptographic overlap.

Myers, Adam, interview with Thomas Rid, Washington, DC, 27 March 2017; see also Crowdstrike, “Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units,” Washington, 22 December 2016.

<sup>17</sup> Bittman, Ladislav, *The KGB and Soviet Disinformation. An Insider’s View*. Washington: Pergamon-Brassey’s, 1985, p. 50–51.

<sup>18</sup> Russian intelligence agencies evolve their tradecraft at a fast pace, making it hard for network defenders to keep up with. Just this week, news emerged that APT29 is abusing Tor Hidden Services for controlling attacks against that likely target US government and think tanks. See FBI, “Vulnerabilities and Post Exploitation IOCs for an Advanced Persistent Threat,” Washington, DC: FBI Cyber Division, 11 May 2016, p. 3. For background, Eduard Kovacs, “OnionDuke APT Malware Distributed Via Malicious Tor Exit Node,” *Security Week*, 14 November 2014. More recently: Matthew Dunwoody, “APT29 Domain Fronting With TOR,” Fireeye, 27 March 2017.

<sup>19</sup> As many as 15 percent of Twitter accounts may be bots, which amounts to almost 50 million “users.” One recent research project observed “a growing record of malicious applications of social bots.” See Onur Varol et al, “Online Human-Bot Interactions: Detection, Estimation, and Characterization,” *Social and Information Networks*, arXiv:1703.03107, 27 Mar 2017.

<sup>20</sup> Agayants, quoted in Bittman, *The KGB and Soviet Disinformation*, p. 70.