

Commentary: Russian Active Measures and the 2016 Hack

The Cipher Brief
December 20, 2017

John Sipher
Former Member, CIA's Senior Intelligence Service

They say the definition of insanity is doing the same thing over and over and expecting a different result. Funny, that. The Soviet and Russian intelligence services have been doing exactly the same thing against us for decades, but this time it finally worked.

Why?

As most Americans are aware by now, the Kremlin undertook a series of actions to interfere in our presidential election in 2016. The sum of these aggressive measures – some overt and some covert – were designed to sow confusion, aggravate political polarization, stir racial tensions, discredit the American democratic system, weaken the U.S. relationship with its allies and hurt Hillary Clinton as a presidential candidate. These type of activities – called “active measures” in the Russian foreign policy playbook – are nothing new.

Putin and the Kremlin see the U.S. as their main enemy and use all the tools of state power to hurt the U.S. and weaken the West. Kremlin doctrine holds that political warfare is as important as military action in weakening and defeating an enemy. Active measures are asymmetric political actions meant to influence an adversary – the art of having your enemy think what you want him to think.

Active Measures include propaganda, media manipulation, disinformation, deception, use of forgery, funding of extremist and opposition groups, spreading conspiracy theories and rumor, cyber-attacks, espionage and even assassination. “Political Influence” is considered the most important part of an effective active measures campaign. Political influence involves using spies and cooperative contacts to directly promote Russian interests inside adversary countries. These individuals secretly working on behalf of Russia are called “agents of influence.” It is not clear if the Russians secured spies inside the Trump campaign, but they certainly tried.

Of course, none of this is new. The Russians, and Soviets before them, have been spreading disinformation and attacking American interests with these asymmetric tools since the 1940s.

A Soviet disinformation campaign in the 1980s attempted to spread the theory that the AIDS virus was created by the Pentagon as part of an out-of-control secret biological warfare program, according to [The New York Times](#).

Prior to the use of social media platforms to spread disinformation, the Russians used a then-favorite mechanism to spread the false story – placing an article in an English-language

newspaper in India. Then, using spies and collaborators, the KGB helped the article get picked up by increasingly credible media outlets, with the goal of eventually having it picked up by the western press. Once in circulation, the information would complicate efforts to tell truth from fiction, and sow distrust with western leaders. As explained by Dr. Thomas Boghardt in the [Times story](#), “The Soviets intuitively understood how the human psyche works.” He said they identify internal strife, point to inconsistencies and ambiguities in the news, fill them with (fake) meaning, mix in some accurate information, and “repeat, repeat, repeat.”

A 1979 Russian disinformation effort led to the death of American diplomats in Pakistan. When an early Al-Qaida-like group seized the Grand Mosque in Mecca and called for the removal of the ruling Saudi family, the Russians spread an incendiary rumor that American troops were involved in the take-over of the holy site. The hoax inflamed Muslim fears and incited protests around the world. A mob in Islamabad stormed the U.S. Embassy and burned it to the ground, killing U.S. diplomats.

There is no shortage of such examples. During the Cold War and beyond, the KGB spread numerous false stories of U.S. assassination attempts, planted forged documents, stoked racial discord and provided support to violent groups. Former KGB officer Sergei Tretyakov’s book “Comrade J” claims the Kremlin invented and disseminated the notion of nuclear winter in an effort to discredit U.S. missile deployments in Europe.

In Latin-America, the Kremlin circulated allegations that wealthy Americans were buying up and butchering poor children in order to use their body parts for transplants. The story even made it into the U.S. press. More recently, the Kremlin orchestrated a coup attempt in Montenegro, stoked anti-EU sentiments in Britain in the lead-up to the BREXIT vote, spread rumors of rapes by migrants in Germany, and added fuel to the fire of secession discussions in Spanish Catalonia.

As troubling and painful as these and other covert campaigns were, none have had the strategic impact that we witnessed in 2016. Why?

Social media: Although the Russians were up to their old tricks in 2016, the internet and social media provided new means to weaponize information. The Russians no longer need to rely on a small army of spies to spread propaganda and lies from Indian tabloids. Facebook and other venues do the work for them. An algorithm directs fake news to those who might be interested, and our “sharing” does the rest. We learned in 2016 that an emotional meme can have as much impact as a well-researched article in the mainstream media.

We’ve seen the enemy and he is us: The success of the Russian attack was proportional to the ferocity of the partisan divide in the U.S. As former CIA and NSA Director Michael Hayden commented in a recent “Atlantic” article, “covert influence campaigns don’t create divisions on the ground, they amplify them.”

In 2016, the dysfunctional U.S. political environment was dry tinder for the Russians. A single match led to a wildfire. Most successful active measures campaigns are not born of elaborate schemes cooked up from whole cloth. Instead, they are often a series of opportunistic and tactical

operations that come together due to a unique set of circumstances. In the case of the 2016 attacks, it wasn't particularly difficult to turn Americans against each other.

Indeed, in 2016, it appears there was a disconnect between the effort, thought and pre-planning expended to carry out the attack, and its resulting impact. The hack of the Democratic National Committee (DNC) was no more than a phishing expedition by a known Russian proxy. As an intelligence operation, it required minimal effort, displayed no professional elegance and was poorly hidden. If the Russians knew ahead of time how important the material would be to the success of their plan, it would have been child's play to have stolen it without getting caught.

However, once they had it in hand and realized how well it fit with other material from separate operations, it was too tempting not to use it. In this sense, the hack of the DNC and subsequent publication of the material in WikiLeaks is surely one of history's best examples of enormous impact from minimal input.

Putin's rage: The scale and brazen nature of the 2016 attack can be attributed in part to the personality of Vladimir Putin. For Putin, years of resentment against the U.S. for perceived disrespect and betrayal, culminating in 2012 street riots in Moscow and the publication of the Panama papers, created a convenient target in Hillary Clinton and the Washington foreign policy establishment. Putin's animus toward Clinton increased his tolerance for risk, and willingness to show his hand.

U.S. wasn't prepared: By 2016, the years of focus on terrorism and the Middle East had fooled many into assuming that the Russians were no longer a threat. Greater familiarity with the Russian threat led to a better defense during the Cold War. Indeed, proximity to an aggressive Russia helped our European allies be better prepared to counter Russian propaganda and fake stories in 2015 and 2016. They Russians tried similar methods in France, Germany and elsewhere but did not have the same level of success.

Collusion? According to Russian doctrine, a successful active measures campaign relies on enlisting spies and "agents-of-influence" to help focus the attack. The Russians certainly called on all available resources to insure success, and like any good intelligence service, continued to seek new spies. Were the Russians aided by collaborators inside or around the Trump campaign, or inside our social media companies? We don't know. If not, it would be a rare covert campaign that did not leverage human sources.

We do know, however, that countering similar attacks in the future will be made more difficult by the failure to hold Russia to account, and by Trump administration attacks on the media and national security institutions. Weakening our defenses does not seem a wise course of action.

Russian-born British journalist and author Peter Pomerantsev has written how Putin has used lies, disinformation and an assault on the media to disable the ability to hold the powerful to account in Russia. As Pomerantsev explained in *Nothing is True and Everything is Possible*, the goal of Russia's dirty tricks "is to confuse rather than convince, to trash the information space so the audience gives up looking for any truth amid the chaos." When the waters have been so fouled, the population develops a hardened cynicism and no longer tries to discern truth from

fiction. No set of facts is better than another, all politicians are the same, no country is better than any other. As they say in Russia, “everything is PR.”

Let’s hope that U.S. institutions prove stronger than those in Russia. For, even if President Donald Trump does not fully understand the damage he is doing, the Russians do, and will seek exploit our weaknesses in the future.