BROOKINGS

Order from Chaos

The next Russian attack will be far worse than bots and trolls

Alina Polyakova Thursday, March 22, 2018

Editor's Note:

In the very near term, writes Alina Polyakova, technological advancements in artificial intelligence and cyber capabilities will open opportunities for malicious actors to undermine democracies more covertly and effectively than what we have seen so far. An all-out attack on Western critical infrastructure seems inevitable. This piece originally appeared on Lawfare.

On March 15, the Department of Homeland Security together with the FBI announced that Russian government hackers infiltrated critical infrastructures in the U.S.—including "energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors." According to the DHS-FBI report, malicious Russian activities have been ongoing since at least March 2016. The Russian malware, which has been sitting in the control systems of various U.S. utilities, allows the Russians to shut off power or sabotage the energy grids. And they have done it before: The same malware that took down Ukraine's electrical grid in 2015 and 2016 has been detected in U.S. utilities. The potential damage of a nationwide black out—let's say on Election Day—would be significant, to say the least. And while Russian trolls and bots have captured public attention, they are already yesterday's game. As I write in a recent Brookings paper, the future of political warfare is in the cyber domain.

The disinformation tools used by Moscow against the West are still fairly basic: They rely on exploiting human gullibility, vulnerabilities in the social media ecosystem, and lack of awareness among the public, the media, and policymakers. In the very near term, however, technological advancements in artificial intelligence and cyber capabilities will open opportunities for malicious actors to undermine democracies more covertly and effectively than what we have seen so far. Increasingly sophisticated cybertools, tested primarily in Ukraine, have already infected Western systems, as evidenced by the DHS-FBI report. An all-out attack on Western critical infrastructure seems inevitable.

In the West, Russia's cyberattacks so far have been at the service of its disinformation operations: stolen data used to embarrass individuals, spin a narrative, discredit democratic institutions and values, and sow social discord. This was the pattern Russian operators followed in the United States, France, and Germany during the countries' 2016–17 elections. Hacking email accounts of individuals or campaigns, leaking that stolen information using a proxy (primarily WikiLeaks), and then deploying an army of disinformation agents (bots, trolls, state controlled media) to disseminate and amplify a politically damaging narrative. Such cyber-enabled interference falls below the threshold of critical infrastructure attacks of significant consequence that could result in "loss of life, significant destruction of property, or significant impact on [national security interests]."

The nightmare of cyberattacks crippling critical infrastructure systems still has the sound of science fiction to most Americans. But in Ukraine, this nightmare is real. As the laboratory for Russian activities, Ukraine has seen a significant uptick in attacks on its critical infrastructure systems since the 2013–14 Maidan revolution. A barrage of malware, denial of service attacks, and phishing campaigns bombard Ukraine's critical infrastructure environments on a daily basis. In December 2015, a well-planned and sophisticated attack on Ukraine's electrical grid targeted power distribution centers and left 230,000 residents without power the day before Christmas. The attackers were able to override operators' password access to the system and also disable backup generators.

The Ukrainian government attributed the attacks to the Russian hacking group called Sandworm. "BlackEnergy," the same Sandworm malware that caused the blackout in Ukraine, has been detected in electric utilities in the United States. Ukraine's "Christmas attack," as the 2015 blackout has come to be known, is the worst known attack on critical infrastructure systems. And Ukraine's systems—defended by a combination of firewalls, segmented access, two-factor authentication, and manual controls—were more secure at the time of the attack than those in the United States. Thanks to Soviet-era manual switches, the blackout lasted only a few hours—a luxury that most U.S. utilities don't have.

Russian attacks on Ukraine have already spilled over to Europe and the U.S. In June 2017, the so-called "NotPetya" virus, which originated in a targeted attack on Ukraine's accounting systems, spread to 64 countries and affected major international companies, logistical operators, government agencies, telecommunication providers, and financial institutions. The name, NotPetya, referred to the disguised nature of the attack; it appeared as a previously launched ransomware attack (Petya) but was in fact designed to destroy and delete information systems in Ukraine. In effect, NotPetya was a cyber form of "maskirovka," or tactical deception, often used in Soviet military operations to mislead and deceive adversaries about the true source and intention of an attack. In February 2018, the U.S. attributed NotPetya to the Russian military.

Ukraine's experience with Russian election hacking should also be a call to action. Widely used electronic voting machines in the U.S. have weak security and software full of easily exploitable loopholes. Many were purchased after the contested 2000 presidential elections, which means that some localities are relying on 20-year-old software in the upcoming 2018 midterms. At the 2017 Defcon hacker conference, attendees were tasked with breaking into a range of American voting machines either by finding vulnerabilities through physically breaking into machines or gaining access remotely. The hackers did so in less than two hours. Participants managed to breach every piece of equipment by the end of the gathering. U.S. intelligence officials confirmed earlier this year that Russian hackers infiltrated election systems in seven U.S. states (Illinois, Alaska, Arizona, Texas, California, Florida and Wisconsin) and gained access to voter registration rolls. DHS officials testified in June 2017 that Russians probed at least 21 states' voter registration systems but did not necessarily "get through the door." While no evidence has emerged that the Russians altered the voter data in the 2016 elections, they could pull the trigger at any time. As with utilities, the Russians have effectively planted cyber bombs that they can detonate when the political timing is right.

The next Russian attack on the U.S. could be massive in scope and debilitating in its effects. It will make social media bots and trolls look benign by comparison. It could be as straightforward and easily traced back to Russia, or it could be far more ambitious. For example, "WannaCry," the May 2017 ransomware attack that crippled hospitals in

Western Europe by exploiting a vulnerability in Microsoft Windows, was based on an exploit originally identified by the National Security Agency. The exploit was leaked and a hacker group known as the Shadow Brokers published the detailed code online in April 2017. After the attack was unleashed, the U.S. identified North Korea (not Russia) as responsible for WannaCry in the fall of 2017. WannaCry presents a potential new threat vector: Malicious actors (Russia, China, etc.) hack Western intelligence agencies and leak the information to third parties (Shadow Brokers or others) that then post the exploits publicly, allowing other bad actors around the world to use the tools for whatever ends. In this case, it is more difficult to definitively lay the blame on a single actor, which constrains the West's ability to respond.

The next Russian attack on the U.S....will make social media bots and trolls look benign.

Computational propaganda, or the "use of algorithms, automation, and human curation to purposely distribute misleading information over social media," is also evolving. Advancements in artificial intelligence (AI) and machine learning will enable malicious actors to spread disinformation faster and in a more targeted manner. Detecting automated accounts, often called "bots," will also become more difficult as these accounts appear increasingly human—they will be able to adapt to human reactions, tailor messaging, and exploit human emotions. In a cyber attack, disinformation campaigns by human like users will be used to mislead the public about the nature and severity of the threat, magnifying the chaos and amplifying the damage.

The United State and Europe seem ill-equipped to deter and respond to online disinformation attacks, much less a cyber attack on critical infrastructure. A year-and-a-half after the elections, the U.S. has not come up with a comprehensive response to Russian interference. Sanctioning the Russian troll factory, as the Trump administration recently did, will not deter a future attack. In fact, according to the

DHS-FBI findings, Russian cyber attacks have only increased since the elections. Sanctions, while an useful policy tool, should be part of much larger deterrence arsenal that should include defensive and offensive measures. In its constant probing, Moscow is testing U.S. resolve to respond, and the weakness of that response so far has undoubtedly served as a lesson for other bad actors—Iran, North Korea, China—seeking to undermine Western societies. As a first step, the U.S. and European countries, should develop a strategy of deterrence against political warfare with clearly defined consequences for adversarial actions. This strategy should have overt and covert operational components, including public statements by political leaders, intelligence communications to convey the potential costs to adversaries, and an increase in covert operations aimed at identifying adversaries' vulnerabilities. The most important ingredient in crafting such a strategic and coordinate response is political will from the top—something sorely missing in the U.S. today.

Order from Chaos

A how-to guide for managing the end of the post-Cold War era. **Read all the Order from Chaos content »**