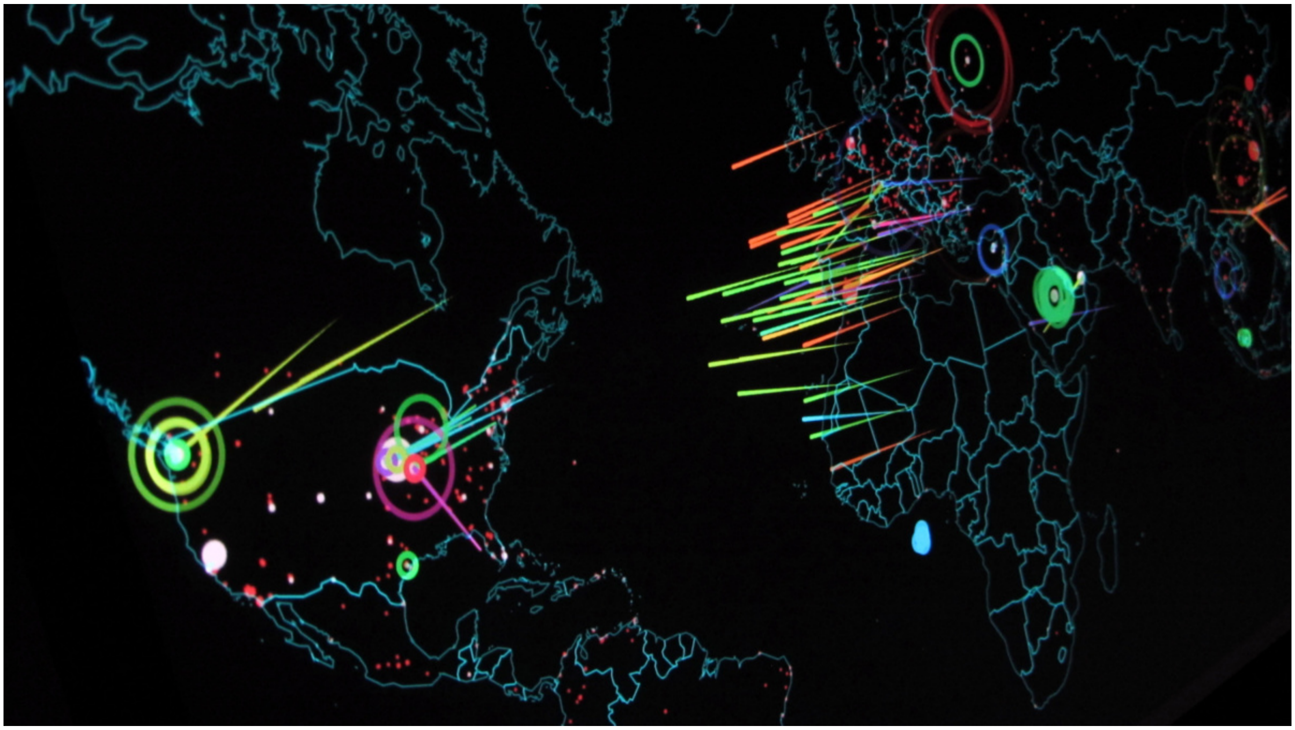
2018-01-28

Russias Ultimate Weapon Might Be Cyber

Jasper, Scott

S. Jasper, Russias Ultimate Weapon Might Be Cyber, The National Interest, January 30, 2018
http://hdl.handle.net/10945/57095

Russia's Ultimate Weapon Might Be Cyber



Printer friendly version

A recent report prepared for the Senate Foreign Relations Committee unveiled President Putin's motivations for an Asymmetric Assault on Democracy in Russian and Europe. His asymmetric use of covert means for political ends became evident in Ukraine. Cyber operations employed together with information operations across conventional, economic and political sectors have created a societal siege mentality for Ukrainians. Yet Kremlin interference also threatens the peace and stability of the United States and Europe. Given the potential impact of cyber operations on the international community, are their use by Russia rational or irresponsible?

The term "rational" denotes behavior appropriate to specified goals in the context of a given situation. The primary Russian goal is restoring its position as an independent Great Power through every possible means. In an energy dependent economy constrained by Western sanctions and low oil prices, cyber operations are not a significant burden viewed in macroeconomic terms. They are asymmetric weapons in the Russian arsenal that may achieve political utility through the capability to covertly alter an adversary's policy. Putin seeks to undermine the democracies on his country's periphery in states that attempt integration with the European Union and NATO. A series of cyber incidents align closely with this geostrategic objective and current Russian doctrine.

Cyber operations disrupt, deny, degrade or destroy information as well as computer systems and networks. Russian proxies attempt to influence the policy of other states in a desired direction. The most prominent hacktivist group during the Ukraine revolution was CyberBerkut, a front for the Russian Main Intelligence Directorate (GRU). In the Ukrainian presidential elections in 2014, CyberBerkut compromised the Central Election Commission by disabling real-time vote counting and posting false results which appeared on Russian television stations. The malware detected on that cyber attack also was used by APT28, another GRU-affiliated proxy that hacked the Democratic National Committee in 2016 during the presidential campaign in the United States. Subsequent leaks of selected emails represented the Russian attempt to influence American voters.

In December 2015, Russia demonstrated a willingness to employ cyber operations forkinetic effects by disrupting the Ukrainian power grid. The substations of three electric companies were remotely disconnected, which left 225,000 customers without power for several hours in the dead of winter. The attackers also intensified the disruption by flooding call centers with fake messages to block access by customers reporting outages. The hackers possessed the ability to cause physical damage to breakers to permanently take power stations offline. This attack indicated a rational decision by Russia because cyber operations achieved its political objective of demonstrating the brazen intention to disrupt Ukrainian society without irreparable harm or loss of life.

Ukrainian government officials blamed the Russian security services for the power outages, while researchers linked malware to the Sandworm group responsible for hacking government systems in Ukraine. Anonymity offers a means for achieving political utility by furnishing plausible deniability while attaining strategic objectives. Lately the Russian-associated Dragonfly group has compromised energy firms in both the United States and Europe. This group accessed operational systems, meaning it gained the capability to control these systems if it they decide to do so. While election tampering leads to chaos in internal affairs, positioning itself to disrupt the energy sector gives Russia the means to push back against U.S. trade sanctions for nefarious activity.

Ukrainian government officials blamed the Russian security services for the power outages, while researchers linked malware to the Sandworm group responsible for hacking government systems in Ukraine. Anonymity offers a means for achieving political utility by furnishing plausible deniability while attaining strategic objectives. Lately the Russian-associated Dragonfly group has compromised energy firms in both the United States and Europe. This group accessed operational systems, meaning it gained the capability to control these systems if it they decide to do so. While election tampering leads to chaos in internal affairs, positioning itself to disrupt the energy sector gives Russia the means to push back against U.S. trade sanctions for nefarious activity.

According to the report submitted to the Senate, Russia was intending to “weaken Ukraine to the point that it becomes a failed state, rendering it incapable of joining Western institutions.” The Central Intelligence Agency attributed the NotPetya cyberattack that disrupted computers in Ukraine during June 2017 to GRU operatives. The mock ransomware wiped data at banks, energy firms and an airport. NotPetya installed through tax and accounting software updates from a Ukraine site but also spread to the United States and Europe. Maersk, the world’s largest container ship company, reported a $300M loss due to a significant interruption. The American pharmaceutical giant Merck suffered similar losses but more concerning was their shutdown of production of the pediatric vaccine GARDASIL for HPV and adult Hepatitis B vaccine. While the goal of NotPetya might have been rational for the political utility of covertly disrupting Ukrainian financial systems, the result was irresponsible because patients will die from a lack of vital vaccines.

The Russian use of cyber operations to gain political influence is unlikely to go away in the near future. Investigators recently found that APT28 was establishing phishing sites to target the U.S. Senate. The efforts following the U.S. presidential campaign to change the calculus in Russian decisions on cyber operations through economic sanctions, diplomatic expulsions and compound closures failed. Normative considerations could impose reputational costs that affect self-restraint, primarily from rational calculations of interest. Although no such costs have been imposed by the international community for Russian cyber operations against Ukraine. Thus, Russian expectations of loss from cyber operations is too small to alter behavior. In the mind of the decision makers in Russia, cyber operations are rational because they have become a preferred asymmetric means to achieving political utility, regardless of allegations that they are irresponsible.

*Scott Jasper teaches at the Naval Postgraduate School and is the author of*Strategic Cyber Deterrence: The Active Cyber Defense Option*. You can follow him*@ScotJasper*.*