



Calhoun: The NPS Institutional Archive
DSpace Repository

NPS Scholarship

Publications

2017-08-05

Russia sanctions are insufficient: use active cyber defense

Jasper, Scott

The Diplomat

S. Jasper, "Russia sanctions insufficient: use active cyber defense," The Diplomat, (August 5, 2017), 3 p.

<https://hdl.handle.net/10945/55408>

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>

THE | DIPLOMATRead The Diplomat, **Know the Asia-Pacific**

Russia Sanctions are Insufficient: Use Active Cyber Defense

“A new approach is needed to shape views of the costs and benefits of cyber attacks.”

By **Scott Jasper**

August 05, 2017

Regrettably **the bill signed** by U.S. President Donald J. Trump imposing new sanctions on Russia for alleged meddling in the 2016 election is insufficient to change the behavior of this malevolent actor. After all, three years of sanctions by the United States and European Union have caused **severe economic hardship** but have not prevented Russian backing of insurgents in eastern Ukraine, where President Petro Poroshenko called recent days some of **the bloodiest this year**. Russia continues to deny official involvement in the fighting, just as Russian President Vladimir Putin did at the G20 Summit regarding the U.S. election, while asking Trump for **proof and evidence**. Although Putin has claimed **Russian Patriots** may have acted on their own, in the same way that his special forces disguised as **Little Green Men** on the streets of Crimea were supposedly local volunteers. A more effective option than economic sanctions is active cyber defense, which offers real-time detection and stopping of network intrusions combined with the use of legal actions to offset such threats.

Famed social scientist Thomas Schelling once remarked that deterrence is to prevent action by fear of consequences. Obviously, the efforts of the Obama administration to deter Russia by imposing limited sanctions and diplomat expulsions in December for **cyber-enabled activities** did not instill any sense of fear. Granted, any effort to deter adversaries from operating maliciously in cyberspace is constrained by their abilities to remain nameless and act without prosecution. What is more, motivations that involve political objectives, national ideology, or even financial gain are not easily discouraged.



081203-N-2147L-390 NORFOLK, Va. (Dec. 3, 2008) Sailors on the watch-floor of the Navy Cyber Defense Operations Command monitor, analyze, detect and defensively respond to unauthorized activity within U.S. Navy information systems and computer networks. — Released (Text by U.S. Navy)

Image Credit: **Mass Communications Specialist 1st Class Corey Lewis**, U.S. Navy

In contrast, active cyber defense halts activity after an intrusion and thwarts actor objectives. This approach makes it more difficult to conduct attacks and provides added forms of punishment. Moreover, it increases the inclination of adversaries for restraint notwithstanding their actual identity or number. Both the technical capability and legal viability of active defense withstand attacks *inside* networks as well as disrupt actors *outside* networks.

The Tallinn Manual on Cyber Operations permits nations to take actions called countermeasures in response to a violation of sovereignty or intervention in internal affairs, including cyber operations to change electronic balloting in elections. Additionally, it does not prohibit nations from turning to a private firm to conduct cyber countermeasures on their behalf. The controversial term “hack back” applies when victims of cyber attacks act on their own initiative to stop an ongoing attack. Today the vexing problem is that most cyber attacks do not meet the threshold and capacity for authorized government responses. Therefore hack backs should be considered for use by licensed private companies with official approval and under supervision, for example by the U.S. Department of Justice under legal exceptions.

Choices to disrupt an actor are taken on a sliding scale – from enabling attackers to steal fake files or embedding beacons to reveal their location or infiltrating their networks to alter, retrieve or delete stolen data. French authorities watched Russian cyber activity during the presidential campaign of Emmanuel Macron. Technicians established **false email accounts** and filled them with phony documents which forced the Russian hackers to waste their time. Recognition that use of more aggressive measures may allow organizations to exact revenge, inflict damage on innocent computers, and run the risk of out-of-control counter strikes creates the need for internal solutions.

Therefore, active cyber defense also defeats cyber threats along their attack process using integrated and automated capabilities within institutional bounds. Such capabilities work. In the breach of the Target Corporation discount chain immediately before the holiday shopping season in 2013, Eastern European criminals stole 40 million credit and debit card numbers. They collected and transmitted some 11 gigabytes of data to servers outside the country, to include one in Russia. The LightCyber Magna platform has the capability to detect large uploads and movement of data. In the hacking of the Democratic National Committee last year, after two separate Russian intelligence-affiliated hacker groups installed malware, similar active defense capabilities could have stopped them before damaging emails were stolen.

Attempts to prevent North Korean cyber attacks with measures to deny benefits or impose costs have also failed. In the attack on Sony Pictures Entertainment in 2014, the North Korean hackers freely collected emails and movies for months before releasing a destructive virus. Once the intrusion was linked to Pyongyang, the U.S. Department of the Treasury imposed penalties on North Korea; the same response that has not prevented numerous nuclear and missile tests. Active cyber defense is needed to frustrate and punish a range of malicious actors regardless of their origin or intentions.

The National Security Agency determined that **North Korea was behind** the WannaCry Ransomware attack in May that locked down more than 200,000 computers in 90 countries, including 16 hospitals in the United Kingdom. WannaCry also shut down **the Honda plant** northwest of Tokyo and Nissan Motor worldwide. However, Symantec reported that no technical evidence indicated that the criminal group Lazarus, which was linked to the attack, was working at the **behest of a nation state**. Regardless of who did it, active cyber defense has proved its worth in systems featuring installed capabilities. For instance, the Palo Alto Networks Traps platform blocked WannaCry malware execution before any files could be encrypted.

Putin signaled **a significant escalation** in the Russian response to U.S. sanctions, ordering cuts of 755 people at U.S. diplomatic missions and **seizing U.S. diplomatic properties**. To end this saga, a new approach is needed to shape views of the costs and benefits of cyber attacks. Active cyber defense can withstand attacks by any perpetrator by multiple detectors together with automated internal actions. However, government-licensed responses by the private sector would also increase capacity to prevent such actions. Active defense has credibility to block cyber attacks before they achieve their objective, preventing another occurrence which prompts the inevitable response of *prove it* from a defiant voice in the Kremlin.

*Scott Jasper teaches at the Naval Postgraduate School. His most recent book, **Strategic Cyber Deterrence: The Active Cyber Defense Option**, published by Rowman & Littlefield, is available in both paperback and on Kindle. Follow @ScotJasper*
