



T Rid, SAIS, 1619 Massachusetts Ave NW, Washington, DC 20036

The Honorable Ron Wyden
United States Senate
Washington, DC 20510-3703

9/14/18

Subject: Congressional Cybersecurity

Dear Senator Wyden:

I understand the Federal Election Commission (FEC) is looking for expert analysis on the threat foreign hackers pose to Members of Congress and senior United States Government officials. I write to provide you my professional assessment in hopes that you will pass it on to the FEC.

By way of background, I am a Professor at Johns Hopkins University's School of Advanced International Studies and an expert on cybersecurity. Before moving to Washington D.C. last year, I was a Professor of Security Studies at King's College in the United Kingdom. My recent work focuses on identifying and analyzing the threats posed by cyberattacks. My piece "How Russia Pulled off the Biggest Election Hack in US History," from October 2016, has received widespread media attention. In March 2017 I testified in front of the Senate Select Committee on Intelligence on election interference.

For-profit criminals go after Americans with identity theft, ransomware, spyware, phishing attacks, impersonal fraud, or other scams. But senior executive branch officials and Members of Congress face additional, targeted threats from sophisticated, persistent, and often well-funded adversaries. The motivations of these hostile actors vary widely. Some seek sensitive information to embarrass or disrupt the workings of our government, while others are probing for weaknesses in our nation's defenses. Tactics vary widely, too, from using highly sophisticated technical intrusion capabilities, to borrowing tactics from criminals (e.g. phishing and spyware). Whatever the technical route, and whatever the motivation, no country has a larger target surface than the United States.

Thomas Rid
Professor of Strategic Studies

The Paul H. Nitze School of Advanced International Studies
1619 Massachusetts Avenue NW Washington, DC 20036
rid@jhu.edu <https://ridt.co>
<https://sais-jhu.edu>

Tip of the Iceberg

In 2016, hackers working for the Russian government broke into a range of targets, including the network of the Democratic National Committee, the email account of Senator Hillary Clinton's presidential campaign manager John Podesta, and former chairman of the Joint Chiefs Colin Powell. These widely publicized breaches are only the tip of a vast iceberg. These hacks are widely known today because the emails stolen from these accounts were subsequently weaponized and used as part of a campaign to influence the outcome of several elections — most publicly, the Presidential race between Donald Trump and Hillary Clinton, but also House races in Illinois, New Hampshire, New Mexico, North Carolina, Ohio, and Pennsylvania.¹ Senator Lindsey Graham also reported that his campaign's email was successfully compromised.²

While the 2016 hacks were a watershed moment, they are only the most visible and disruptive instances of this wider threat to American democracy. In 2008, the Obama and McCain presidential campaigns were both reportedly compromised by hackers working for the Chinese government. These cyber operations had all the hallmarks of traditional espionage. The hackers reportedly stole “massive amounts of internal data from both campaigns — including internal position papers and private emails of key advisers in both camps,” which were quietly exfiltrated.³

Critically, we know about these attacks because the hacked information was deliberately leaked, or because the hackers were sloppy, or unlucky, and got caught. For example the hacking against White House Chief of Staff John Kelly's phone appears to have only been discovered because it caused his device to malfunction. It is likely that we only know a fraction of the total number of successful hacks. Without a systematic effort to track cyberattacks against American officials, many of the most sophisticated digital operations, particularly those conducted for espionage rather than in aid of influence operations, are likely to remain hidden.

Personal Devices and Accounts: Unprotected but Highly Targeted

The wave of hacking and hacking attempts against United States officials are not limited to agency servers and official, government email accounts. **Every major hacked-and-leaked email account during the 2016**

¹ “Democratic House Candidates Were Also Targets of Russian Hacking,” *The New York Times*, Dec. 13, 2016

² “Graham: Russians hacked my campaign email account,” CNN, Dec. 14, 2016

³ “Chinese hacked Obama, McCain campaigns, took internal documents, officials say,” NBC News, Jun 6, 2013.

election interference campaign was a non-government (personal or campaign) account — many of the documents that Russian fronts claimed came “from the DNC” in fact did not come from the DNC, but from personal email accounts. These accounts are outside the official security perimeter of the U.S. government, yet contain highly sensitive information about officials’ activities, private communications, family life, finances, and movements. Personal accounts are often much softer targets because the user determines the security settings, not cybersecurity professionals.

As a result, hackers working for foreign powers (as well as so-called ‘hacktivists’) have zeroed on the non-official accounts of current and former officials. These include: White House Chief of Staff John Kelly (personal phone), former CIA Director John Brennan (personal email), former DNI James Clapper (personal email, phone accounts), and former FBI Deputy Director Mark Giuliano (personal email).

[Protecting Senators at Work and at Home](#)

Private-sector intelligence reports show that several Senators and their staff have been targeted by advanced, persistent cyber attacks beginning in June of 2017.⁴ Critically, adversaries targeted probably more personal accounts than official accounts.

It is my expert opinion that these reports only scratch the surface of the advanced cyber threats faced by Senators, House members, senior executive branch officials and important political staff. Further, it is clear that our most aggressive and dangerous adversaries do not limit their targeting to official accounts and devices and why anybody would think so is beyond me. But because personal accounts and devices are at an even greater risk.


The personal accounts of Senators and their staff are high-value, low-hanging targets. No rules, no regulations, no funding streams, no mandatory training, no systematic security support is available to secure these resources. With no one forcing them to improve their personal cybersecurity and little expert assistance available, it’s unsurprising that many elected officials have bad personal cybersecurity. In this regard, elected politicians indeed represent average Americans — like most people, they reuse passwords, don’t bother with two-factor authentication, and regularly open attachments they receive via email on their own devices. That may not sound bad, but it is. Poor personal cybersecurity habits may not create serious problems for the average American, or indeed endanger

⁴ “Update on Pawn Storm: New Targets and Politically Motivated Campaigns,” Trend Micro, 12 January 2018.

national security. The average American, after all, does not have foreign intelligence services trying to break into their email account and smartphone.

Tragically, we all now recognize that physical threats against Members of Congress follow them beyond the grounds of the Capitol. So too cyber threats follow Members to whichever accounts and devices they use. If anything, hackers are likely to target the digital resources that are the least protected, which will frequently be a personal account or device. It would therefore be prudent as well as urgent to encourage and support efforts to increase the security of Senators' personal devices and accounts.

Sincerely,


Thomas Rid
Professor of Strategic Studies
Johns Hopkins University/SAIS