LAWFARE

CYBERSECURITY

Cybersecurity in the 2017 National Security Strategy

By **Michael Sulmeyer** Tuesday, December 19, 2017, 2:00 PM

DayZero: Cybersecurity Law and Policy

Today, the Trump administration released its National Security Strategy. This piece will address one narrow element of the document: cybersecurity. It's a hot topic, but compared to North Korea's nuclear-tipped missile program, Iran's destabilizing activities in the Middle East, China's muscle-flexing across almost all domains of statecraft, and Russia's growing role as a spoiler around the world, I thought the National Security Strategy wouldn't have much to say about cybersecurity. I was wrong.

The administration should be given relatively high marks for the document's cybersecurity components—especially for recognizing the breadth of the threat and that it's going to take more than the help desk to fix it. Admittedly, that's a pretty low bar. But National Security Strategy documents are not known as documents where big policy innovation occurs. Instead, the best you can usually do is articulate the broad contours of the main threats to national security coupled with some rough themes about what the government will do to make things better. Here, the administration does not isolate "the cyber" to the sidelines; instead, by talking about cyber issues throughout the document, the administration shows an understanding that cyberspace is a critical part to practically every aspect of national security.

This feels like a more thorough treatment of cybersecurity as a core national-security concern than we've seen in the past. Before, for Democrats and Republicans, the priorities have been stopping the theft of U.S. intellectual property and hacking of U.S. businesses and protecting federal networks and critical infrastructure. How? Concepts like "deterrence" are often—maybe too often—borrowed from the Cold War and grafted onto this more complex domain. And there is the historical love affair with information sharing. While this National Security Strategy emphasizes similar objectives, it goes beyond them and devotes appropriately little space to deterrence and information sharing.

Before going further, a brief appeal to a refrain I try to hit often: Try to keep the politics out of cybersecurity. No matter whether you watch Jesse Watters or Rachel Maddow, we should try to examine documents like the National Security Strategy objectively as possible. The question we need to ask is: Will the principles and priorities that the document articulates keep the country safe? The answer can't come in a puff piece or a hit job. Just taking the National Security Strategy released today at face value, my initial reaction is that yes, it keeps the United States on a positive trajectory to better (if gradual) cybersecurity.

Here are some of the cyber-related highlights:

- Not surprisingly, the document is tough on China. Indeed, the administration calls out China for "cyber-enabled economic warfare." The language is more assertive than in past National Security Strategies, but the theme of pounding the Chinese for their theft of critical U.S. intellectual property is not new.
- More surprisingly, it is also tough on Russia. The National Security Strategy labels Russia's actions in cyberspace as "destabilizing" and asserts that Russia "uses information operations as part of its offensive cyber efforts to influence public opinion across the globe."
- The largest—if predictable—disappointment is that the document does not prioritize the protections of elections in the U.S. from cyber threats. To be fair, it acknowledges that adversaries are attacking America's institutions and that part of being resilient as a nation "includes the ability to withstand and recover rapidly from … threats to … our democratic system." And it states that "actors such as Russia are using information tools in an attempt to undermine the legitimacy of democracies." But the document stops well-short of articulating the cybersecurity issues around the 2016 election and how to make sure those events don't repeat themselves.
- I am surprised by the tone around attribution. While I was in the Defense Department, I had come to believe that the U.S. government had a pretty good sense of who was doing what in cyberspace. Of course, no one—not then, and not now—would be against better attribution. But I would have thought that the document would lead off by emphasizing that the United States possesses solid insight into this, so those who would try to hack and hide should think twice. Indeed, White House homeland security adviser Tom Bossert was very direct in his assertion on Tuesday that North Korea was the perpetrator behind last May's WannaCry attack.

The 2017 National Security Strategy is built around four pillars. (There is also a short concluding section about how these four pillars play out across six regions around the world.) They are:

- "Protect the American People, the Homeland, and the American Way of Life"

- “Promote American Prosperity”
- “Preserve Peace through Strength”
- “Advance American Influence”

Cybersecurity features prominently in the first three.

The first pillar holds the administration’s views on how cyberspace activities will contribute to U.S. efforts to defeat “Jihadist” terrorists. Terrorist safe havens include the internet, and the document makes explicit mention of needing to address the “going dark” problem, although it recognizes that working with private industry is important to solving it. There is also a section on transnational criminal organizations, which the administration acknowledges can be used by some state adversaries “to conduct unattributable cyber intrusions, sabotage, theft, and political subversion.” (Charley Snyder and I wrote about the Justice Department’s indictment earlier this year of Russian criminals, who evidently had links to the Russian government, for hacking Yahoo.)

There is also a dedicated section in the first pillar entitled “Keep America Safe in the Cyber Era.” Readers will find familiar language here about threats to critical infrastructure, federal networks and the like. But there is an important evolution from the previous administration’s strategy: To prioritize risk, the Trump administration will focus only on six sectors: national security, energy and power, banking and finance, health and safety, communications, and transportation. By contrast, the Obama administration grappled with at least 15 “critical” infrastructure sectors. Surely, there is some rhetorical consolidation, but nonetheless, six is much more practically defensible than 15.

This section is also where readers will find the familiar refrains about more secure federal networks, deterring and disrupting bad guys, and improving information sharing. But what caught my eye was a small section on “layered defenses.” Here is the key excerpt:

[T]he U.S. Government will work with the private sector to remediate known bad activities at the network level to improve the security of all customers. Malicious activity must be defeated within a network and not be passed on to its destination whenever possible.

Think of this like “trickle-down cybersecurity.” Sure, it is important that users and businesses have good cybersecurity standards in place. But we get more bang for our buck if the government and large service-providers can block threats before they reach businesses and operators of important systems. (To their credit, Britain is putting something like this in place right now through their National Cyber Security Centre.)

Pillar two, entitled “Promote American Prosperity,” contains the predictable fighting words about China’s theft of intellectual property. This prose can be found in the “Promote and Protect the U.S. National Security Innovation Base” subsection and characterizes China’s actions as “cyber-enabled economic warfare.” What the document lacks is any new principle or commitment for how to prevail in this kind of “warfare.” We read that “the United States will prioritize counterintelligence and law enforcement activities to curtail intellectual property theft by all sources and will explore new legal and regulatory mechanisms to prevent and prosecute violations.” Yet this is not new, as the Obama administration tried similar approaches to curtail China’s IP theft. Perhaps the reference to regulatory mechanisms has some additional meaning, but this is a section that I hope will be the subject of more public discussion in the months ahead.

What’s worth noting in pillar two is that in the introductory and narrative prose, there is an explicit connection made between cybersecurity and prosperity. Yes, cybersecurity. Not just “the digital economy,” “innovation,” and other buzzwords. At the start, they write that “protection from persistent cyberattacks [is] needed to support America’s future growth.” And more emphasis on security, not just connectivity: “Economic and personal transactions are dependent upon the “.com world,” and wealth creation depends on a reliable, secure Internet.” This is important language for businesses, universities, and other institutions to process, not because wealth creation is such a core objective, but because cybersecurity risks are a clear and present danger to our economy.

Pillar three, “Preserve Peace Through Strength,” is where readers will find tough language about Russia’s activities in cyberspace. The document affirms that Russia is indeed investing in a suite of new military capabilities, including “destabilizing cyber capabilities.” In a not-so-thinly veiled reference to Russia’s recent use of information operations to sway elections, the National Security Strategy adds that “Through modernized forms of subversive tactics, Russia interferes in the domestic political affairs of countries around the world.” It is a positive development that this document doesn’t sugar-coat Russia’s aggressive acts in cyberspace.

Countering Russian efforts also drives a rather creative section on “information statecraft.” (That this notion of online statecraft is discussed in pillar three probably explains why cyber issues are absent from pillar four, which more explicitly considers diplomacy.) I don’t want to rehash the full page-and-a-half, but I would encourage readers to read this section (pages 34 and 35 of the document), because it captures the new challenges our competitors are posing to U.S. interests through their use of information. It contains an illustrative but not hyperbolic reference to artificial intelligence, and frames the “ideological information campaign” waged by terrorists as one of the central threats the United States must address. It also puts some responsibility on media and internet companies to do their part in limiting how their platforms are used and abused to promote hateful values. The Obama and Bush administrations struggled with the same phenomena. This will be another area where the Trump administration can hopefully share some additional details in the months ahead.

There's also an important posture of realism in this section about our own cyber capabilities relative to those of our competitors. The administration subtly acknowledges that the United States does not dominate today's cyberspace when it states that:

The spread of accurate and inexpensive weapons and the use of cyber tools have allowed state and non-state competitors to harm the United States across various domains. Such capabilities contest what was until recently U.S. dominance across the land, air, maritime, space, and cyberspace domains.

That kind of humility reflects important developments over the last several years, including the damage of the Snowden disclosures and our growing vulnerabilities to cyberattack due to our reliance on technology even as our adversaries incrementally improve their exploitation skills. To be sure, this is not a main argument from the Trump administration. But to the extent that future policy reflects the fact that cyberspace is much more of a contested domain today than it once was, we will be on grounded footing.

There is also a dedicated subsection on cyberspace, including a helpful articulation of the need to invest in capabilities that facilitate a "rapid response" to cyberattacks. The most sophisticated and "cool" hack loses value for decision-makers in a crisis if it takes months to employ. To that end, one area where I would have liked to see a reference to U.S. cyber forces was in the section about military readiness. I think the drafters missed an opportunity to stress the need for Cyber Command's maturing Cyber Mission Force must be a force that is ready to fight. While that may be an obvious point, rhetoric matters in documents like this one. While U.S. strategists intuitively recognize that the readiness of conventional and nuclear forces is one of the most critical aspects of military policy, the readiness of our cyber forces should be seen in a similar light. Finally, some explanation of how "overmatch"—this document's general characterization of the force posture and armament strategy it will pursue—applies to U.S. cyber forces would be a useful addition.

***

I conclude where I started: There's a lot more in the 2017 National Security Strategy about cybersecurity than I expected. Yes, there are some important shortcomings, like not mentioning the cybersecurity of elections. Make no mistake: That's a big one. But other than that, the drafters of this National Security Strategy deserve credit for threading an incredibly complex needle, as fighting for column inches on cybersecurity is never easy when there are so many other pressing threats in the world. This document gives sufficiently thorough treatment to how cybersecurity issues today permeate almost every issue of American national security, including economic, military, and even democratic security. To the drafters' credit, there's no bluster or fearmongering about cybersecurity that comes through in these sections.

One final note: I take comfort that the drafters of this National Security Strategy did not let Russia off the hook. In fact, they were quite tough on Russia, especially on their cyber and information operations. Those who deny Russia's aggressive intentions would be wise to read some of the many passages that make the case very clear that the Putin's interests are definitely not the same as our own. This does not mean that cooperation will not be possible one day. This document's language about Russia's aggression, especially in cyberspace, is now U.S. policy, affixed with President Trump's signature. If there was any doubt before, this document clears up that such concerns are anything but #fakenews.

Topics: Cybersecurity

Dr. Michael Sulmeyer is the Belfer Center's Cyber Security Project director at the Harvard Kennedy School. He recently concluded several years in the Office of the Secretary of Defense, serving most recently as the Director for Plans and Operations for Cyber Policy. He was also Senior Policy Advisor to the Deputy Assistant Secretary of Defense for Cyber Policy. In these jobs, he worked closely with the Joint Staff and Cyber Command on a variety of efforts to counter malicious cyber activity against U.S. and DoD interests. Previously, he worked on arms control and the maintenance of strategic stability between the United States, Russia, and China. As a Marshall Scholar, Sulmeyer received his doctorate in Politics from Oxford University, and his dissertation, "Money for Nothing: Understanding the Termination of U.S. Major Defense Acquisition Programs," won the Sir Walter Bagehot Prize for best dissertation in government and public administration. He received his B.A. and J.D. from Stanford University and his M.A. in War Studies from King's College London.