"The GOP Blueprint for Cybersecurity in the 2016 Presidential Election"

Austen D. Givens
Assistant Professor of Cybersecurity
Utica College
adgivens@utica.edu

WORKING DRAFT PAPER

Cite as: Austen D. Givens, "The GOP Blueprint for Cybersecurity in the 2016 Presidential Election," Occasional Working Paper, January 26, 2016.

VER. 1/26/16

Cybersecurity is today a central component of the federal government's broader national security strategy.[1] But it is unclear how the leading contenders for the GOP presidential nomination would manage cybersecurity policy from the White House. At the time of writing in January 2016, the leading Republican contenders in the race—Donald Trump, Ted Cruz, Marco Rubio, and Jeb Bush—have said virtually nothing about their approaches to cybersecurity. It is also not apparent how a GOP vision for cybersecurity in 2016 would differ from, or overlap with, the Obama administration's approach to cybersecurity. All of which begs the question: what would a conservative vision for cybersecurity in 2016 look like?

A compelling conservative vision for cybersecurity would combine a sober assessment of cybersecurity threats with a steady adherence to conservative principles. Four key focus areas stand out. First, the United States should develop a powerful cyber deterrent capability against nations like China, Iran, and Russia. Second, we must retaliate aggressively, consistently, and publically against nations and non-state actors that purposefully break into, and damage or destroy, U.S. computer networks. Third, conservatives should emphasize that cybersecurity begins with individual awareness of cyber threats and individual acceptance of personal responsibility for cybersecurity. And fourth, the federal government must further embrace the private sector as a co-equal partner in cybersecurity efforts, using creative financial incentives to induce voluntary public-private sector cooperation.

Cyber deterrence can dissuade state and non-state actors from breaking into, and harming, U.S. computer systems. The logic underpinning cyber deterrence theory is that states will probably refrain from breaking into U.S. computer systems if they know that they will face a devastating cyber counter-attack for having done so. For government organizations like the National Security Agency, this means that continuing to build innovative cyber weapons, and cultivating previously-unseen exploits of electronic vulnerabilities, known as "zero-days," could help turn bad actors away from the idea of breaking into our computer networks.

There is a vigorous discussion in academic circles today regarding whether or not deterrence theory could prove as effective in the cyber domain as it did in the nuclear domain during the height of the Soviet-U.S. nuclear arms race.[2] Yet it is difficult to see how building up

[1] https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf
[2] For example, see Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (August 2013): 365–404; Jon R. Lindsay, "Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattacks," *Journal of Cybersecurity* 0, no. 0 (November 2015): 1–15 (advance open access).

a formidable cyber deterrence capability could be harmful at this point, given the steady, predictable stream of data breaches suffered by government agencies, businesses, and citizens each day.

For instance, there is significant evidence that China and Russia have made cyberattacks and network intrusions key components of their foreign policy and economic development strategies.[3] China's new FC-31 fighter jet is a dead ringer for Lockheed Martin's F-35 Joint Strike Fighter, and it appears that China based the FC-31 design on stolen F-35 plans that it obtained through a hack of U.S. Department of Defense networks in 2009.[4] With tensions at a low simmer between the United States and China in the South China Sea, the U.S. Navy faces the prospect of having its own stolen technology used against it in the form of the knock-off Chinese FC-31 fighter jet. This scenario illustrates well the extent to which China's theft of virtual intellectual property can have real-world consequences for U.S. national security. It also underscores the compelling need for a strong deterrent capability in cyberspace.

When cyber deterrence fails, however, the United States must be ready and willing to fight back publically against cyber intrusions. Failure to retaliate openly invites further network intrusions. To its credit, the Obama White House has shown some willingness to counter-attack. For example, in 2014, as Sony Pictures prepared to release *The Interview*, a movie that openly mocked North Korean strongman Kim Jong Un, Sony Pictures suffered a cyberattack that wiped eye-popping amounts of data from the company's servers and led to the disclosures of embarrassing emails sent among top Sony executives.[5] U.S. intelligence officials expressed confidence that hackers working for the North Korean government were behind the attack on Sony Pictures.[6] Just days later, North Korea's already limited access to the Internet was mysteriously and completely shut off.[7] The Obama administration did not claim responsibility for making North Korea "go dark." But Obama himself said in a press conference that the U.S. government would respond "proportionately" to the Sony Pictures attack.[8] One is left to connect the dots.

---

[3] For official assessments of Chinese and Russian online espionage, see http://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.
[4] http://www.wsj.com/articles/SB124027491029837401; http://www.smh.com.au/national/china-stole-plans-for-a-new-fighter-plane-spy-documents-have-revealed-20150118-12sp1o.html
[5] https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/
[6] https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/
[7] http://www.wsj.com/articles/north-koreas-internet-goes-dark-1419295353
[8] http://www.wsj.com/articles/north-koreas-internet-goes-dark-1419295353

The trouble is that the decision to counter-attack is inevitably modulated by other political considerations. The challenge for conservatives, then, is to show willingness to temporarily push aside these political considerations in the name of better cybersecurity.

For example, the delicate, multi-layered tensions in the U.S.-China relationship mean that the United States has strong incentives not to counter-attack against China's cyber intrusions. In May 2014, the U.S. Department of Justice indicted five Chinese army officers, accusing them of hacking into manufacturing and utility firms with operations in the United States.[9] Later that year, however, the United States inked a trade deal with China that would slash tariffs on U.S. and Chinese imports of hi-tech goods.[10] In April 2015, President Obama signed an executive order authorizing the U.S. Treasury Department to impose financial sanctions and freeze the assets of foreign actors who consistently carry out cyberattacks against the United States.[11] And in September of last year, Chinese President Xi Jinping and U.S. President Barack Obama reached an agreement in which they each committed not to engage in economic espionage against one another.[12] Security experts immediately labeled the accord worthless.[13]

It is reasonable to assume that the United States' lack of consistency in fighting back openly against cyber intrusions has emboldened our adversaries in their cyberattack campaigns--specifically Russia, China, and Iran, which have stepped up the number, duration, and severity of their cyberattacks on U.S. and western targets in recent years. But by publically making clear the consequences of cyberattacks, and taking equally public steps to fight back against them, the U.S. cyber deterrent will be strengthened.

Accepting personal responsibility for one's actions—or inaction—is a bedrock principle of American conservatism. Consistent with this idea, a conservative platform for cybersecurity should place the onus for cybersecurity not on government, but on individuals. For example, utility companies in particular have been slow to enhance the security of aging industrial control systems—computers and software that regulate processes like electrical currents in power substations or the flow of water through dams. The Republican candidate for president can encourage utility companies to adopt a more pro-active approach to cybersecurity, not through

[9] http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor
[10] http://www.ft.com/intl/cms/s/0/9a1804d6-6950-11e4-9eeb-00144feabdc0.html#axzz3yGvJgsUL
[11] http://thehill.com/policy/cybersecurity/237581-obama-declares-cyberattacks-a-national-emergency
[12] http://www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/
[13] For example, see http://nationalinterest.org/feature/why-the-us-china-cyber-spying-ban-will-inevitably-fail-14219 and http://www.reuters.com/article/us-usa-cybersecurity-idUSKCN0RT1Q820150930.

taxes or regulation, but by simply changing the market forces and incentives that go into utility owners' spending decisions. If it is clear to business owners that there is no government funding available to mop up the effects of massive network breaches and data theft, then they are more likely to take measures to enhance their organizations' cybersecurity on their own.

In this same spirit, the 2016 GOP presidential nominee should embrace the private sector as a co-equal partner in cybersecurity efforts. The Obama White House has tried, unsuccessfully, to brow-beat tech companies into cooperation. For instance, following the June 2013 revelations by Edward Snowden of a massive NSA spying campaign, Google Executive Chairman Eric Schmidt, Yahoo CEO Marissa Mayer, then-Twitter CEO Dick Costolo, and Facebook COO Sheryl Sandberg, among others, flew to Washington to meet with Obama and to push back against government pressure to surveil their customers.[14] In early 2016, the President's national security team, including FBI Director James Comey and Director of National Intelligence James Clapper, went to California to enlist tech companies to help the government combat extremism more effectively on social media.[15] Naturally, tech companies are reluctant to bend to this government pressure, for fear of losing customers who might see them as spying on behalf of the government.

Yet there is another, potentially more effective way to enlist tech firms in the fight against online extremism: by making cooperation with the government financially attractive for tech firms. Tax breaks, loosened regulations, and doling out access to government-backed research and development funding are three easy ways that a Republican president can make public-private sector collaboration more enticing for Silicon Valley executives. Hard financial incentives are more likely to induce the private sector cooperation that the federal national security community seeks. And the reasons for this are straightforward. Financial incentives can help tech executives to maximize value for their shareholders; arm twisting by government leaders does not. Monetary sweeteners are easy ways to strengthen cybersecurity and to repair the now strained relationship between the White House and Silicon Valley.

To be sure, our next President faces monumental challenges in U.S. cybersecurity. And, like so much in government, there are no easy fixes or solutions to the challenges that the next President will confront. For the eventual 2016 GOP presidential nominee, however, there is a

[14] http://www.wsj.com/articles/SB10001424052702304403804579264501539629002
[15] http://www.wsj.com/articles/top-u-s-officials-to-meet-with-tech-ceos-on-terror-concerns-1452195796

clear path forward for cybersecurity—one that remains true to conservative principles, while assessing candidly the cyber threats that the United States faces.