THIRD WAY
National Security

Announcing the Third Way Cyber Enforcement Initiative

In Greek mythology, the dog Laelaps was put on earth to relentlessly pursue its quarry and was immortalized by Zeus as a constellation in the sky in relentless pursuit of the fox Teumessian, famed never to be caught. The gap between hunter and prey seemed impossible to close. In cybersecurity, we face a similar situation, but our Laelaps needs help. In the face of a massive and dangerous cybercrime wave and cybersecurity threats, **Third Way is launching a new non-partisan initiative aimed at closing the cyber enforcement gap through a relentless pursuit of malicious cyber actors.**

The Federal Bureau of Investigation (FBI) receives approximately 300,000 cybercrime complaints per year. These attacks range from the mundane intrusion to attacks on the Federal Reserve. The FBI has calculated that just the reported crimes cost victims more than $1.4 billion,[1] though the economic effect is estimated to be much higher, at between $57 billion and $109 billion annually in the United States.[2] Meanwhile, state sponsored actors are attempting to break into key American cyber systems daily. Yet, we estimate that the cybercrime enforcement rate is less than 1%.[3] Compare that to the property crime enforcement rate, where law enforcement closes nearly one in five reported cases.[4]

Looking at the cyber enforcement gap, it's no wonder that vast majority of cyberattacker(s) feel they can operate with impunity with little fear of getting caught. We need a national strategy to transform law enforcement, enabled by diplomacy, to close the cyber enforcement gap. Third Way's initiative will aim to change that by closing the cyber enforcement gap and creating a comprehensive strategy for the United States to identify, stop, and punish global cyberattacker(s).

Initiative Overview

A week before the tragic terrorist attacks on 9/11, senior national security officials in the Bush Administration finally met to discuss the threat of al-Qaeda.[5] This meeting came after an eight month delay, during which Richard Clarke, the White House's counterterrorism chief under Presidents Clinton and Bush had become increasingly frustrated at the lack of urgency to address the threat.[6] In preparation for the meeting Clarke sent a memo to his boss, then-National Security Advisor Condoleezza Rice, urging "policymakers to imagine a day after a terrorist attack with hundreds of Americans dead at home and abroad and ask themselves **what they could have done earlier**."[7]

With terrorism, the threat was known, attacks against Americans were continuing, and the problem wasn't going away. In retrospect, the failure to fully grapple with the threat of terrorism and how the US government should respond before the attacks left the nation unprepared and reeling, scrambling to hastily adopt policies, many of which had to be jettisoned or modified as

their effectiveness came into question. These early—and avoidable—policy missteps have had enduring consequences for the credibility of the US government both domestically and abroad.

Once again, the United States is under attack, this time in the digital domain through a cybercrime wave. Yet, the nation is facing the very real prospect that it will repeat the mistakes of 9/11 in failing to be prepared for a different threat – that of cyberattacks. Every day, malicious cyberattacker(s) threaten America's government institutions, civil society, businesses, and people, inflicting extraordinary damage.[8] Secretary of Homeland Security Kristjen Nielsen recently warned that "an attack of that magnitude [on 9/11] is now more likely to reach us online than on an airplane. Our digital lives are in danger like never before."[9] Director of National Intelligence, Dan Coats, recently testified that the "warning lights are blinking red again" but this time it is cyberattacks against our digital infrastructure.[10]

And even though most cyberattacks do not cause the kind of visible, physical, and human impact that al-Qaeda inflicted upon us seventeen years ago, the pervasiveness of these attacks, the range of impacts, and the scope of vulnerability is much broader. We are amidst a national cybercrime wave. Yet, the government has failed to match this threat with the political will and human and fiscal resources needed to counter it. This crisis will not be solved by simply using a military-centric approach and increased network protection. Without empowering law enforcement and our nation's diplomats to pursue cybercriminals, the massive and dangerous cyber enforcement gap that exists will continue. Again we must now ask ourselves, what can policymakers do earlier to address this threat?

Third Way's Cyber Enforcement Initiative marks the first ever non-partisan public policy initiative dedicated specifically to developing and implementing a comprehensive enforcement strategy against global cyberattacker(s). In partnership with a distinguished Advisory Board comprised of former US government law enforcement, cybersecurity, and diplomatic officials, industry representatives, and experts, Third Way will seek to develop and push for policy action aimed at enhancing the government's cyber enforcement abilities. We also aim to change the narrative around cybersecurity so there is a more robust conversation around identifying, stopping, and punishing attackers through domestic and international cooperation and not just one blaming the victims of attacks.

The goals of this Initiative require such a radical re-envisioning of the government that it cannot be resolved in a single report, or single year, but must take dedicated effort over a sustained period of time to achieve the results we seek.

The Cyber Enforcement Initiative

Simply put, here is the change we seek: the United States must institute a comprehensive cyber enforcement strategy that can sufficiently identify, stop, and punish global attackers. In order to develop this strategy we must: 1) change the mindset that punishing the attackers is futile; 2) assess the current strengths and weaknesses of the current enforcement architecture, and 3) create a robust conversation around developing effective policy changes necessary to transform the government's response and rebalance it to one that prioritizes all tools in America's cybersecurity toolbox.

Change the Mindset

First, in order to change the mindset that punishing the attackers is futile, we must acknowledge

the reasons the futility exists. Third Way's own analysis of the data on enforcement actions taken against cybercriminals alone, as highlighted in *To Catch a Hacker*, demonstrates the enforcement rate remains drastically low in comparison to the rate of attacks. Acting with anonymity or perceived anonymity and aided by technology, these malicious cyber actors operate at a level of impunity unseen amongst most other forms of crime. Further, the relative ease of access to technology tools allows an attacker to scale attacks against individuals he or she's never seen in countries they may have never visited. Those seeking to track the hacker face barriers in digital forensics, network ownership, and legal jurisdiction – both domestically and internationally. All of these things require the cooperation of multiple entities to solve the problem.

This futility is also driven by a sense that enforcement actions cannot have an impact when it comes to attackers who are sponsored or sanctioned by America's nation-state adversaries as a tool to target the United States. In these cases, it is true that it may be very difficult to successfully capture and prosecute those individuals involved or alter their behavior. Yet, there have been a number of cases where the US government has had success in arresting and extraditing cyberattacker(s) from these countries.[11] Even in cases where physically getting the attacker may not be possible, enforcement actions, which include sanctions, can serve as an important basis for further diplomatic action that can be taken by the United States and our allies to punish the attackers and their sponsoring countries for their actions.

As the 9/11 Commission observed of the pre-9/11 status quo, "Government agencies also sometimes display a tendency to match capabilities to mission by defining away the hardest part of their job. They are often passive, accepting what are viewed as givens, including that efforts to identify and fix glaring vulnerabilities to dangerous threats would be too costly, too controversial, or too disruptive."[12] Like this pre-9/11 state, the government agencies that work on prosecuting and sanctioning cyberattacker(s) have largely worked within the bureaucratic status quo, not thinking strategically about how to improve the government's ability to bring multiple agencies together in cooperation to identify, stop, and punish attackers.

Assess Our Capabilities

Next, we must develop an accurate picture of the strengths and weaknesses of current US government efforts to identify, stop, and punish the attacker. Without such a baseline, the government will not be able to determine areas of needed strengthening to make progress and risks committing precious resources to ineffective policy approaches. Recently released government reports[13] and strategies[14] do little to map out the details as to how the government intends to close the cyber enforcement gap. Not only do we need to measure the rate of enforcement, but also to assess the training, workforce management, organization, international cooperation and capacity building, and regulatory incentives and disincentives to effective enforcement.

Develop and Promote Policies

Finally, over the next several years, Third Way will explore and develop policies to establish a comprehensive US enforcement strategy to identify, stop, and punish global cyberattacker(s). We will amplify the perspectives of former policymakers and experts to develop innovative policy solutions aimed at improving efforts to change the calculus and behavior of the human attacker. Through this initiative, we will develop policy proposals and push for legislative changes in

collaboration with congressional champions that will measure and enhance the government's efforts to catch and punish attackers. Through these policy changes, we aim to rebalance America's approach to cybersecurity to one that puts America's law enforcement and diplomats at the forefront not just the military. Supported by a non-partisan Advisory Board comprised of leading thinkers on these issues, Third Way will push the US government to establish a comprehensive cyber enforcement strategy and close the cyber enforcement gap.

Through these efforts, we aim to change the status quo narrative around cybersecurity. All too often when a cyberattack hits government or the private sector, the first response is to blame the victim for letting themselves be attacked. Under no other crimes do we want this to be the accepted prevailing narrative. We want to shift this narrative to one in which the onus is on finding the attacker and bringing them to justice. Certainly, companies can and must continue to take steps to protect their systems against cyber threats and face consequences for failing to do so. But the government is the only entity with the authority to pursue enforcement actions against cyberattacker(s) and bring them to justice. Therefore, we believe that one of the greatest needs for reform is in this area.

Enforcement actions can inflict heavy punishment individuals in even the most hard to reach places and the gap in the government's pursuit of these actions must be addressed. The national and economic security of America depends on it.

ENDNOTES

1 Federal Bureau of Investigation. "2016 Internet Crime Report," 22 June 2017, pp. 2. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 3 Oct. 2018.

2 United States White House, Council on Economic Advisers. "The Cost of Malicious Cyber Activity to the U.S. Economy," 16 Feb. 2018, pp. 1. https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. Accessed 2 Oct. 2018.

3 See Third Way's report To Catch a Hacker.

4 Federal Bureau of Investigation. "2017 Crime in the United States." https://ucr.fbi.gov/crime-in-the-u.s/2017/crime-in-the-u.s.-2017/topic-pages/clearances. Accessed 24 Sept. 2018.

5 FDCH E-Media. "Transcript: Wednesday's 9/11 Commission Hearings." The Washington Post, 24 Mar. 2004, www.washingtonpost.com/wp-dyn/articles/A20349-2004Mar24.html. Accessed 2 Oct. 2018.

6 Clarke, Richard. "Presidential Policy Initiative/Review-- The Al-Qida Network." National Security Archive, George Washington University, 25 Jan. 2001. nsarchive2.gwu.edu/NSAEBB/NSAEBB147/clarke%20memo.pdf. Accessed 2 Oct. 2018.

7 FDCH E-Media. "Transcript: Wednesday's 9/11 Commission Hearings." The Washington Post, 24 Mar. 2004. www.washingtonpost.com/wp-dyn/articles/A20349-2004Mar24.html. Accessed 2 Oct. 2018.

8 United States White House, Council on Economic Advisers. "The Cost of Malicious Cyber Activity to the U.S. Economy," 16 Feb. 2018. https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. Accessed 2 Oct. 2018.

9 Miroff, Nick. "Hacking, Cyberattacks Now the Biggest Threat to U.S., Trump's Homeland Security Chief Warns." The Washington Post, 5 Sept. 2018. www.washingtonpost.com/world/national-security/hacking-cyberattacks-now-the-biggest-threat-to-us-trumps-homeland-security-chief-warns/2018/09/05/d0045800-b119-11e8-a20b-5f4f84429666_story.html?utm_term=.4432fe0c6072. Accessed 2 Oct. 2018.

10 Barnes, Julian E. "'Warning Lights Are Blinking Red,' Top Intelligence Officer Says of Russian Attacks." The New York Times, 13 July 2018. www.nytimes.com/2018/07/13/us/politics/dan-coats-intelligence-russia-cyber-warning.html. Accessed 2 Oct. 2018.

11 A number of high-profile arrests and extraditions of Russian hackers demonstrates that there are many circumstances where enforcement actions taken against attackers from adversarial nations may be feasible. See for example: Windrem, Robert. "Will Russian Hackers Rounded up by U.S. Snitch on Putin Regime?" NBCNews.com, NBCUniversal News Group, 10 Apr. 2017, www.nbcnews.com/news/us-news/russian-hacker-busted-spain-latest-global-u-s-roundup-n744911. Accessed 2 Oct. 2018.

12 The National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report, 22 July 2004, pp. 352. https://govinfo.library.unt.edu/911/report/911Report.pdf. Accessed 2 Oct. 2018.

13 United States Department of Justice. "Report of the Attorney General's Cyber Digital Task Force." 2 July 2018, https://justice.gov/cyberreport. Accessed 2 Oct. 2018.

14 United States Department of State. "Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats." 31 May 2018. www.state.gov/s/cyberissues/e013800/282011.htm. Accessed 2 Oct. 2018.