THIRD WAY

Taking Action on Cyber Enforcement: Assessing US Legislative Progress in the 115th Congress

by Ishan Mehta and Jayati Dev

Takeaways

The 115th Congress was very active when it came to cybersecurity legislation and its Members introduced 226 bills on the topic. An analysis of these bills showed both hope and opportunity. On the side of "hope," more than half of the bills introduced were bipartisan, including every bill that eventually became law. The polarization that has affected most issues in Washington has not been inflicted upon cyber security legislation. In terms of "opportunity" however, most cyber bills were defensive-minded, focusing on securing networks rather than investigating, finding, and punishing malicious cyber actors. Going forward, Members of Congress have an opportunity to propose bipartisan legislation to improve the number cybercriminals brought to justice.

Here are the main takeaways from the bills introduced last Congress:

- Cybersecurity legislation is increasing from just a handful of bills introduced several Congresses ago to more than 200 in the most recent Congress.
- Only 31 of the 226 bills introduced in the last Congress, and just two of the ten that were signed into law, focused on imposing consequences on the human actors behind cyberattacks.
- Cybersecurity remains a largely bipartisan issue. Half of all legislation introduced, and all ten that were signed into law, had a bipartisan cosponsor.

Introduction

The United States is in the middle of a rising cybercrime wave. The Federal Bureau of Investigation (FBI) received over 300,000 complaints of malicious cyber incidents in 2017, and that represents only a fraction of all incidents.[1] In a report released last year, we estimated that

out of every 1000 malicious cyber incidents, only three incidents see an enforcement action. Third Way's non-partisan Cyber Enforcement Initiative aims at reducing the cyber enforcement gap through the development of innovative policy solutions and by amplifying other efforts by policymakers that share our goals. It is clear that congressional action is needed to measure and enhance the US Government's ability to stop, identify, and punish malicious cyber actors. In this memo we assess the efforts of the 115th Congress to tackle this issue, and we provide insight into the areas that received insufficient attention.

The US Congress has increased its focus on cybersecurity issues over the last two years exhibited through its legislative action.

Congress' increased attention to cybersecurity-related issues can be seen in the increase of bills that were introduced over the last two years by its Members to tackle a broad spectrum of topics. During the 115th session of the US Congress (January 3, 2017 – January 3, 2019), 226 pieces of legislation that primarily or tangentially focused on cybersecurity were introduced by Members.[2] Congress' involvement on the subject is reflective of the rapid growth in technology. The 106th Congress (January 3, 1999 – January 3, 2001) saw only 16 pieces of legislation introduced that focused on cybersecurity.[3] In the 114th Congress, only 22 cybersecurity bills were introduced according to the Congressional Research Service.[4] The rise of congressional action on cyber-related issues over the past few years may also be indicative of the urgency Congress has felt to legislate on this issue after Russia's malicious cyber activity during the 2016 US presidential election.[5]

The 115th congressional session also saw more bills passed by Congress and signed into law on cyber-related issues than ever before. In the 114th Congress, the only cybersecurity legislation passed by Congress was the cybersecurity provisions in the "Consolidated Appropriations Act, 2016" (PL 114-113), which included elements of three separate bills covering information sharing between the government and the private sector, and cybersecurity workforce expansion and improvement. By comparison, the 115th Congress was able to pass 10 pieces of legislation that were signed into law by President Trump including three omnibus bills that each contained multiple cybersecurity measures.

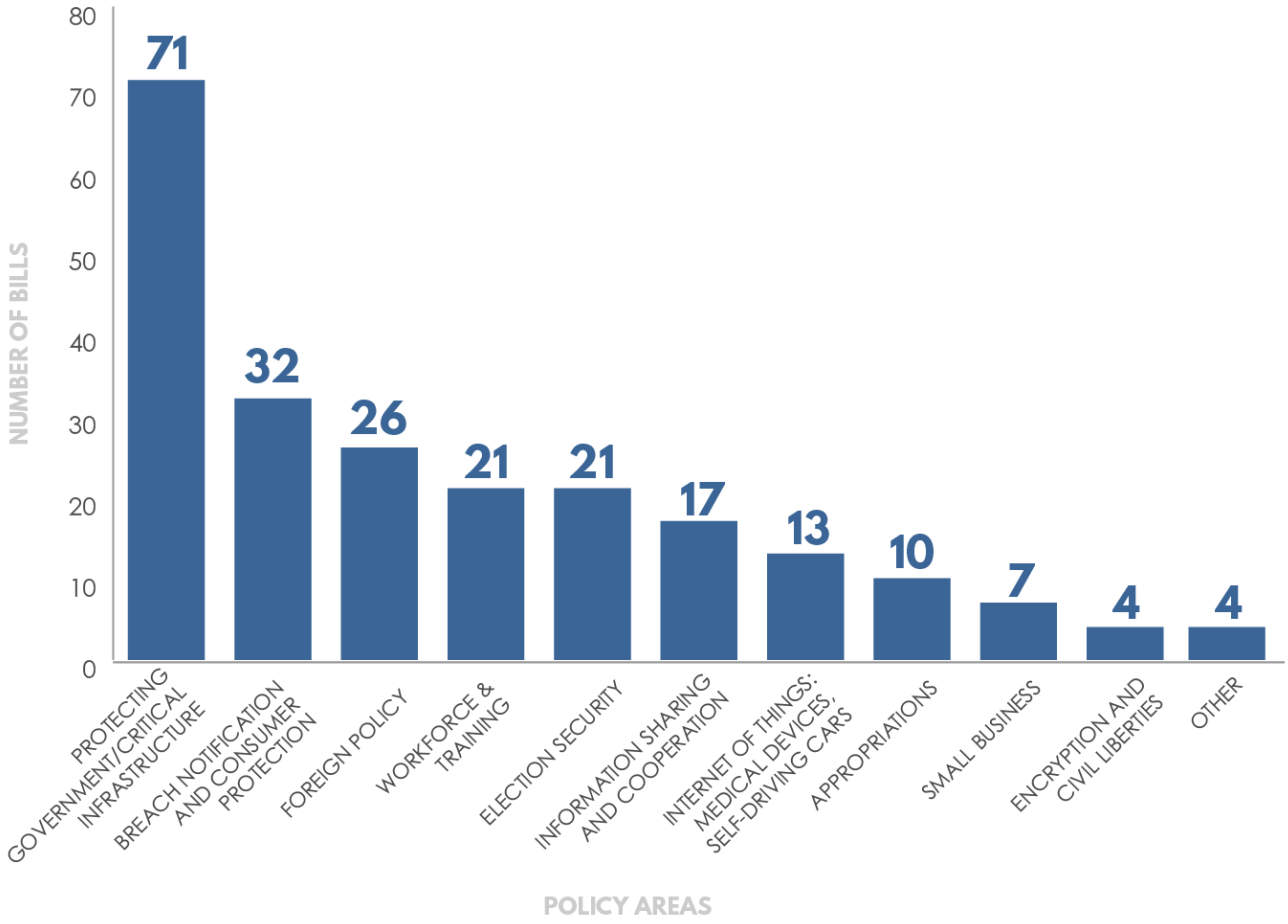
Additionally, there were a number of cyber-related bills that were passed by one chamber, but failed to receive a vote in the other. The House passed 42 bills that did not see a vote in the Senate, while the Senate passed six bills that did not see a vote in the House. This trend is also visible in the 114th Congress, where nine cyber bills passed the House and did not receive a vote in the Senate, and only one bill passed the Senate but did not receive a vote in the House.

Congressional legislation focuses on better cyber-defenses.

Most of the legislation introduced in the 115th Congress was focused on cyber defensive measures and strengthening information systems and networks. Taking a deeper dive into the 226 bills introduced in the 115th Congress, we classified each bill into one of ten different thematic areas related to cyber. The results of that analysis are represented in the graph below.

THIRD WAY

Cybersecurity Legislation in the 115th Congress



This breakdown shows where Congress' priorities lie in its focus on cyber-related issues. For example, 71 bills were introduced in the House and Senate that focus on improving the government's defensive cyber infrastructure. This is the largest area of focus for congressional action. It includes bills that were signed into law like the "SECURE Act" (PL 115-390), which protects the information technology (IT) supply chain for the federal government, and the "NASA Transition Authorization Act" (PL 115-10), which provides funding to develop secure web applications for NASA.

The next highest action area of cyber-related bills that were introduced in the 115th congressional session was consumer protection and breach notification laws. In response to the public outcry to the numerous data breaches of prominent companies like Facebook, Equifax, and others, many Members introduced legislation that focused on putting in place new regulations aimed at preventing data breaches and/or adding reporting requirements for businesses aimed at compelling the private sector to report to the government when they are victims of data breaches. This legislation also focused on granting more protections to users affected in a data breach.

Additionally, Congress introduced a broad category of bills we have grouped under "foreign policy" for their focus on responding to malicious cyber actions perpetrated by nation-states. Twenty-six cyber bills were introduced in this category. Most of these were efforts by Congress to impose sanctions and other penalties on countries like Russia, Iran, North Korea, and China in response to their use of malicious cyber actions, including cybercrime and espionage, and to attempt to deter these further actions against the United States in the future.

The cyber workforce gap has been a concern for the technology industry as well as the federal government. For the public sector, along with cybersecurity professionals required to protect federal IT systems, there is a shortage of law enforcement personnel with the skills to investigate cybercrime. It is estimated that there could be 3.5 million unfilled cybersecurity jobs by 2021.[6] The 115th Congress saw 21 bills introduced to address the issue, one of which, the "Strengthening State and Local Cyber Crime Fighting Act" (PL 115-76), became law in 2017. Amongst other things, the law enables training of state and local law enforcement officers, prosecutors, and judges to handle digital evidence and investigate cybercrime.

After the 2016 US presidential election, we learned that Russian operatives not only hacked the emails of the Clinton campaign and the Democratic National Committee (DNC), but also targeted election infrastructure. They compromised the voter databases and websites of seven states in the run up to the election.[7] Election security was a highly partisan issue in the last Congress, where Democrats have sought additional funding for the states' election security systems, but were thwarted by Senate Republicans.[8]

Of the 226 pieces of legislation introduced, only 10 were signed into law. Some elements of other bills, like the "CLOUD Act" (S. 2383), were enacted as a part of the "Consolidated Appropriations Act, 2018" (PL 115-141). One hundred and twenty-nine of the 226 bills introduced had bipartisan co-sponsorship either in the House or in the Senate. That is well over half of all bills introduced, indicating that, while there are disagreements, cybersecurity remains a more bipartisan issue than most other issues in front of Congress.

All of the 10 bills that were signed into law had bipartisan cosponsors. Three of the 10 were appropriations bills that provided funding to the federal government and three others were focused on improving government IT systems. The "CISA Act" (H.R. 3359) renamed and elevated the National Protection and Programs Directorate to lead the Department of Homeland Security's (DHS) cyber mission in collaborating and sharing threat information with the private sector, as well as federal, state, and local government agencies. The list of all ten bills is below.

	Bill	Policy Area	Sponsor
#	H.R.3359	Other	Michael T. McCaul
Name	Cybersecurity and Infrastructure Security Agency (CISA) Act of 2017		
#	H.R.2810 (S.1519)	Appropriations	Mac Thornberry
Name	National Defense Authorization Act for Fiscal Year 2018		
#	H.R. 1616	Workforce & Training	John Ratcliffe
Name	Strengthening State and Local Cyber Crime Fighting Act of 2017		
#	S. 782	Breach notification and consumer protection	John Cornyn
Name	PROTECT Our Children Act of 2017		
#	H.R. 3243	Protecting government/ critical infrastructure	Gerald E. Connolly
Name	FITARA Enhancement Act of 2017		
#	S.442	Protecting government/ critical infrastructure	Ted Cruz
Name	National Aeronautics and Space Administration Transition Authorization Act of 2017		
#	H.R.3364	Foreign Policy	Edward Royce
Name	Countering America's Adversaries Through Sanctions Act		
#	H.R. 7327 (S. 3085)	Protecting government/ critical infrastructure	Will Hurd
Name	Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE Technology Act		
#	H.R.1625	Appropriations	Edward Royce
Name	Consolidated Appropriations Act, 2018		
#	H.R. 5515	Appropriations	Mac Thornberry
Name	John S. McCain National Defense Authorization Act for Fiscal Year 2019		

THIRD WAY

Despite the increase in congressional action on cyber, there is a concerning gap in legislative focus on cyber enforcement — identifying, stopping, and punishing malicious cyber actors.

Upon analyzing the 226 bills that were introduced in the 115th Congress and the 10 laws that got passed, we noted a concerning lack of focus on policies that would help the US government stop, identify, and punish malicious cyber actors using law enforcement and diplomatic approaches. Most of the legislation that was introduced and passed is aimed at improving government defenses against attacks and resiliency to recover after a major attack. This is a vital component of a comprehensive government cyber strategy, but as we argued in our paper, To Catch a Hacker, defensive efforts need to be balanced with a comprehensive strategy for the US government's efforts bring to justice the humans who perpetrated or ordered the attacks to begin with.

Current efforts are simply not enough. As mentioned earlier, we estimated that for every 1,000 cyber incidents, only three see an enforcement action.[9] Malicious cyber activity costs the US economy up to $109 billion dollars annually.[10] We've seen cyberattacks against critical infrastructure like America's power grid, hospitals, and electoral systems.

Despite this substantial cyber enforcement gap, Congress has not dedicated its legislative efforts to trying to reduce it. Undoubtedly, legislation to secure US government systems are required to prevent malicious cyber actors from accessing them, as are sound data breach laws that hold the private sector accountable for violations. However, a cyber strategy solely built on defense will ultimately fail because a determined attacker will always find a way in. Defensive efforts must therefore be coupled with efforts aimed at demonstrating to malicious cyber actors that they cannot continue to hurt America's governments, businesses, organizations, and people with impunity.

Of the 226 bills that were introduced in the last congressional session dealing with cyber-related issues, only 31 focused on imposing costs on perpetrators. That is barely 14% of all legislation introduced. Only two of the 10 that cyber bills that were signed into law grappled with these issues. The "Strengthening State and Local Cyber Crime Fighting Act" (PL 115-76) funds efforts to train more law enforcement officials, judges, and prosecutors to be adept at handling digital evidence and fight cybercrime. The "Countering America's Adversaries Through Sanctions Act" (PL 115-44) imposes sanctions on nation-states for their cyberattacks on the United States. But other important bills to closing the cyber enforcement gap, such as the "Cyber Diplomacy Act of 2017" (H.R. 3776) to establish an Ambassador for Cybersecurity and corresponding office at the State Department, failed to pass Congress before the 115th congressional session ended.[11] This bill would be critical to ensuring the United States has the proper diplomatic leadership to work with other countries to enhance international cooperation on cyber enforcement. The bill has been reintroduced in the new Congress as the "Cyber Diplomacy Act of 2019" (H.R. 739).

Congress has an opportunity to boost the US government's efforts to reduce the cyber enforcement gap in the 116th Congress with bipartisan support.

Congress should work to lay the foundation for a comprehensive cyber enforcement strategy to better identify, stop, and punish malicious cyber actors in the 2019-2020 116th congressional session. To do that, we have identified a number of key areas where it should focus its legislative action:

1. **Building up law enforcement:** American law enforcement and diplomatic efforts are severely under-resourced to address the growing cybercrime wave. Law enforcement is the primary method to counter malicious cyber activity, and we need to beef up their capacity to narrow the cyber enforcement gap.
2. **Invest in international cooperation and coordination:** The global nature of the cyber threat requires international coordination and cooperation on closing the enforcement gap. Congress should pass the "Cyber Diplomacy Act" (H.R. 3776) to reinstate the State Department Cyber Coordinator's Office and ensure that funding is provided to bilateral and multilateral cyber capacity building efforts.
3. **Establishing comprehensive metrics to measure success:** There is no current baseline of the US government's efforts in this area. Congress should use its oversight role to make federal law enforcement accountable and establish a comprehensive assessment to determine what is working, what might need to be amplified, and what might need to change.

As Director of National Intelligence, Dan Coats, indicated in his testimony in the Worldwide Threat Assessment before the Senate this year, this Administration is lacking a comprehensive strategy to combat malicious cyber activity. In absence of leadership from the White House, the 116th Congress has the opportunity to act with legislation that would help reduce the cyber enforcement gap and boost America's law enforcement and diplomatic efforts to bring malicious cyber actors to justice.

ENDNOTES

1 "2016 Internet Crime Report." 22 June 2017, pp. 17. https://pdf.ic3.gov/2016_IC3Report.pdf. Accessed 25 Dec. 2019.
Newman, Craig A. "When to Report a Cyberattack? For Companies, That's Still a Dilemma." The New York Times, The New York Times, 5 Mar. 2018, www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html. Accessed 25 Oct. 2019.

2 For the purpose of this memo we have relied on the Congressional Research Service's classification to define "cybersecurity legislation." This includes legislation focused on offensive, defensive, and enforcement. It does not include legislation that solely focuses on other digital/cyber issues like privacy, net neutrality, and Internet Access.

3 Legislative Search Results for '106th Congress'." Congress.gov, Library of Congress, 24 Jan. 2019, www.congress.gov/. Accessed 4 Feb. 2019.

4 United States, Congress, Tehan, Rita. Cybersecurity: Legislation, Hearings, and Executive Branch Documents, Library of Congress, 8 Nov. 2018. https://www.fas.org/sgp/crs/misc/R43317.pdf. Accessed 6 Jan. 2019.

5 Hawkins, Derek. "The Cybersecurity 202: Senate Defense Bill Pushes Trump to Get Tougher on Russian Hacking." The Washington Post, 19 June 2018, www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/06/19/the-cybersecurity-202-senate-defense-bill-pushes-trump-to-get-tougher-on-russian-hacking/5b279a0c1b326b3967989b34/. Accessed 16 Jan. 2018.

6 NeSmith, Brian. "The Cybersecurity Talent Gap Is An Industry Crisis." Forbes, 13 Aug. 2018, www.forbes.com/sites/forbestechcouncil/2018/08/09/the-cybersecurity-talent-gap-is-an-industry-crisis/. Accessed 16 Dec. 2018.

7 McFadden, Cynthia, et al. "U.S. Intel: Russia Compromised Seven States Prior to 2016 Election." NBCNews.com, 27 Feb. 2018, www.nbcnews.com/politics/elections/u-s-intel-russia-compromised-seven-states-prior-2016-election-n850296. Accessed 17 Dec. 2018.

8 Demirjian, Karoun. "Senate Republicans Shoot down Extra Funds for Election Security." The Washington Post, 1 Aug. 2018, www.washingtonpost.com/powerpost/senate-republicans-shoot-down-extra-funds-for-election-security/2018/08/01/cac1750a-95a1-11e8-a679-b09212fb69c2_story.html. Accessed 13 Dec. 2018.

9 Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, 29 Oct. 2018, www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 3 Dec. 2018.

10 United States White House, The Council of Economic Advisers. "The Cost of Malicious Cyber Activity to the U.S. Economy." February 2018, pp. 1. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. Accessed 4 Jan. 2019.

11 Johnson, Derek B. "Senate Panel Votes to Revive State Cyber Office." FCW, fcw.com/articles/2018/06/26/cyber-state-senate-office.aspx. Accessed 6 Jan. 2019.