Jacob Dineen

Information Policy

4/19/18

Policy Analysis

**POLICY ANALYSIS ASSIGNMENT**

**Title of the bill:** H.Res.459 — 115th Congress (2017-2018)

**Your summary of the bill**:

With the rise of innovation in the digital landscape coupled with the emergence of the Big Data era, consumer data and privacy has never been more threatened than it is right now. This bill, at its core, suggests an increased devotion, both philosophically and economically, to better prepare America’s youth for the ever-present battles of cybersecurity. Namely, the bill promotes increased exposure to ethical hacking among educational programs to increase awareness and decrease scarcity of cyber-capable professionals in the government, military, and the private sector (Correa). For a bill of this nature to become a law, it must pass be passed by legislation and, occasionally, must be approved by an executive. As noted below in the institutional framework, a bill of this nature may have a challenging time being passed into law. With the heightened awareness on US Intelligence Agencies following breaches of trust and circumvention of existing laws, as exposed by Snowden, nationwide support for a bill that increases surveillance, foreign and domestic, is unlikely to incur.

**Goal of the bill**:

A goal is often a broad strategic or tactical definition of the purpose of a particular piece of legislation, often accompanied by specific objectives that have more tangible performance indicators as measures of progress (Schouwstra). The broad goals of H.Res.459, as partially outlined in my summary above, are an increased awareness and economic response to the growing concerns of cyber-attacks and their corollary effects on the US economy and its private citizens’ personal identifiable information (PII). The main goal of the bill is to act as an active response to ‘large scale breaches’ that continue to plague US consumers and their identities, while also pointedly noting risk to US infrastructure and national security that results as collateral damage to this age of digital warfare (Correa).

**Objectives** **of the bill:**

A more operationalized, granular notion, an objective is often accompanied by performance indicators that derive strategy as to how a goal should be measured, and reached. With this bill, although no specific metrics of success are distinguished, broad objectives are made well known. Specifically, the bill points to the current scarcity and increased demand for cybersecurity positions, suggesting that lessened job openings would be a measurable indicator of the success of the bill’s foundation. Another succinct, demonstrable objective of the bill is to “advance curricula development and teach training in basic cybersecurity for middle and high schools” (Correa). This is fundamentally requesting a bottom up, systemic approach to altering academic curriculums to better prepare America’s youth for the rise in existential, and economic effects of cyber-attacks. The latter objective plays the long game, acting more as a cultural injection than short term solutions focused on increasing current levels of professional aptitude. The main performance indicator, per the bill, is to ‘adequately’ fill the increased demand for cybersecurity positions. A reduction of scarcity in the profession would point to the correlative impact of the bill.

**Methods instruments**

Although the bill summarization of H.Res.459 appears to encompass most viable alternatives, there are some omissions. Namely, the injection of curricula that promotes technological awareness to concepts like ethical hacking and cybersecurity counteracts reports of decline in US educational spending, even in the face of economic prosperity and an increased student population (U.S. News & World Report). Would the US government be more willing to infuse cash into education if it eased the burden of costs in relation to foreign and domestic cyber-attacks? A relatively skimmed over concept in the bill is the picoCTF competition. Expanded upon, and slightly derivative, would be government mandates for private companies to outsource instances of ‘hackathons’ to shore up privacy concerns in their respective software. Companies like Bugcrowd and HackerOne act as intermediaries between companies and white hat hackers to legally expose deficiencies and vulnerabilities in existing software (Miller). Ethical hacking, mentioned in the bill, is the tactical employment of countermeasures to combat adversaries and shore up system infrastructure exposed to penetration – This is the modus operandi of the companies mentioned above. I think about ethical hacking in a comparable manner to generative adversarial networks (Goodfellow), in that you have a discriminator and a generator. The discriminator is the ethical hacker and the adversary is the generator trying to fool the classifier. As the hacker learns new methods to expose systems and algorithms, the white hat becomes better at halting adversarial attacks.

**Activities**

The proposed amendments to the bills, as noted above, would include increased government spending, using national averages as an existing baseline, in exchange for scholastic infusion of technology based solutions to counteract cyber-attacks. This could be inclusive of programming languages being brought into curricula during elementary school, or standardized aptitude tests for prospective college STEM students. Implementing standardized tests would help to ensure that today’s youth are justly prepared for the challenges they’ll see in a real world setting and revoke the notion of government entities hiring personnel just to meet a quota. Prospective cyber-security professionals should be well versed in computer systems and networking, neither of which are currently emphasized at the pre-college level. Perhaps an increase in base salary for educators who are proficient in machine learning and artificial intelligence, along with cyber autonomy would work to sway industry professionals into academia. Additionally, the proposal of a government mandated spending threshold for large consumer data companies, particularly in a similar vein to companies like BugCrowd or HackerOne may be positively rewarded by government institutions. To that point, mandatory training provided by subject matter experts on the meticulous and massive delicacy with which consumer data should be handled could elevate domain knowledge. Lastly, an increased devotion, nationwide, to the idea of diversity in STEM related fields may prove to increase perception. It is said that diversity breeds innovation, and innovation, in this case, could lead to a decline in a hacker’s ability to infiltrate US infrastructure.

**Performance**

Performance can be measured in multiple ways, but I propose two main key performance indicators to measure relative success of H.Res.459 in an objective manner. First and foremost, the cost to the US economy because of cyber-attacks was as high as $109 billion in 2016 (LeFebvre). A downtrend in this number would be suggestive of success, although would not prove a causal relationship. Second, the bill explicitly notes cybersecurity employment openings in the government, and projections for all sectors in the United States. The objective of this bill is to close those positions and to reduce scarcity, at its essence, so a closing of those positions over a 10-year plan, a period long enough to allow for the notion that students engaged in new curricula would be emerging into the US workforce, would prove viable. The filling of job openings suggests urgency, so mandatory aptitude tests for working professionals in the field of cyber -security would counteract deflating credentials in favor of inflating personnel numbers.

**Context, conceptual framework**

In order for a bill of this nature to succeed, assumptions are drawn about what the US population deems important to them. If no physical threat is presented and instead war is conducted on the US through cyber-attacks, there is a thought that urgency is neglected. To that point, the citizens of the United States would have to fully back an ‘us versus them’ mentality, rather than separating themselves from their government. A comprehensive backing of this bill by all parties would assume a propensity geared toward personal privacy and security, and the negation of willfully infused ignorance.

**Institutional framework**

The institutional framework of a country is closely tied with the culture and sophistication of a countries abilities, along with their access to resources. America is a bitterly divided political entity with access to vast technological and militant resources. Any general move by a political party is met with the resistance of the opposing party, insistent that their compass of morality is more in line with American values. For these reason, it is hard to see a future where a systematic adaptation of circumstance is retroactively infused into the academic climate, where some would see it as an over-reach of government power geared toward stopping those at the top from lining their own pockets. The differences of opinion in this country are vast, and without public consensus it is unlikely that a sense of urgency imposed by a government regulation, or bill, will change that culture.

**Evaluation**

Evaluation of any impending successes or failures of this bill will be measured by the key performance indicators noted above, and perhaps an even deeper understanding and cultural impact of the significance of personal identifiable information. Enrollment in college programs geared towards the rise in technological advancement, such as artificial intelligence, machine learning, computer science, data analysis and data mining would suggest an enhanced interest in subject matter pertaining to the ideology of the bill. While analysis would need to be conducted to determine estimated benefits of government spending on ethical hacking preparedness, it would be difficult to argue, in theory, that having more people available to shore up system vulnerabilities would lead to an increase in successful cyber-attacks. Ethical hacking is becoming commonplace in professional settings as a preventative measure, but this bill stresses a sense of urgency that we need to quickly evolve, as a country, to mitigate risk in the short term, and into the future.

**Instructions for the cost-benefit section of your policy analysis**

Reference external excel sheet. The most egregious assumption I make here is that a reduction of cyber-attacks would enhance consumer propensity to engage in the economy – It’s not realistic to think that people care about their PIIs enough to stop spending at a level that would make an impact. 5% is an outrageous estimate, but there may be a small portion of the population that withholds from the retail experience due to worries of data breaches.

**References:**

Correa. “Text - H.Res.459 - 115th Congress (2017-2018): Expressing the Sense of the House of Representatives That the United States Should Support the Development of Programs That Better Prepare Students for Careers in Cybersecurity by Actively Promoting Ethical Hacking Skills.” *Congress.gov*, 19 July 2017, [www.congress.gov/bill/115th-congress/house-resolution/459/text?q=%7B%22search%22%3A%5B%22machine%2Bethics%22%5D%7D&r=2](http://www.congress.gov/bill/115th-congress/house-resolution/459/text?q=%7b%22search%22%3A%5B%22machine%2Bethics%22%5D%7d&r=2).

Ellman, and M. J. “A New Explanatory Model for Policy Analysis and Evaluation.” *By M. C. Schouwstra, M. J. Ellman :: SSRN*, 19 July 2006, papers.ssrn.com/sol3/papers.cfm?abstract\_id=917327.

2U. Information Policy Lectures.

“U.S. Spends Less as Other Nations Invest More in Education.” *U.S. News & World Report*, U.S. News & World Report, [www.usnews.com/news/national-news/articles/2017-09-18/while-rest-of-the-world-invests-more-in-education-the-us-spends-less](http://www.usnews.com/news/national-news/articles/2017-09-18/while-rest-of-the-world-invests-more-in-education-the-us-spends-less).

Miller, Ron. “Bugcrowd Bug Bounty Platform Gets Big Boost with $26 Million Series C Investment.” *TechCrunch*, TechCrunch, 13 Mar. 2018, techcrunch.com/2018/03/01/bugcrowd-bug-bounty-platform-gets-big-boost-with-26-million-series-c-investment/.

LeFebvre, Rob. “Cyber Attacks Reportedly Cost the US as Much as $109 Billion in 2016.” *Engadget*, 16 Feb. 2018, www.engadget.com/2018/02/16/cyber-attacks-cost-up-to-109-billion-2016/.