CYSE 406: Cyberlaw
Writing Assignment 2: H.R. 5760 - Grid Security

Kevin Durand, kdura002

Dear Fellow Virginias from the 26th District,

I am writing today to talk to you about a candidate running for reelection and a measure that he supports, the candidate Tito Canduit is planning to run for The House in 2022. During his previous time as a representative of this great district he was instrumental in pushing and voting for Bill H.R. 5760 (https://www.congress.gov/bill/116th-congress/house-bill/5760), the Grid Security Research and Development act, hereafter mentioned by H.R. 5760. H.R. 5760 represents an advancement in cybersecurity that would seek to further protect our infrastructure from cyber attacks. In the last 4 to 5 years we have seen cyber attacks on a couple different places; these attacks have targeted infrastructure and are a warning sign for what would happen if America remained unprepared. H.R. 5760 might not be the complete solution to cybersecurity, in regards to infrastructure, but it does set a positive precedent for future legislation. By explaining this bill, you will see how effective Representative Canduit is, and how much he will fight for you and the American people if he remains in The House.

H.R. 5760: Grid Security and Development Act.

H.R. 5760, which passed the house in 09/29/2022, represents an approach to dealing with the growing threat of cyberattacks against key infrastructure. There are a number of different elements to this Bill, mostly this is about researching the potential for cyber attacks on our energy based infrastructure and developing security advancements based on that research. The first thing that this law sets out to do is "...to identify cybersecurity risks to information system within…the energy sector…" (116th Congress). What this means is that the bill would incentivize private companies and the federal government to work together to prevent potential attacks on our energy systems and infrastructure. The second main stipulation of this bill is "develop technologies that improve the physical security of information systems…"; this is the most important part of this bill, this has the most impact on our nation. Essentially this bill is not just about research, but it is about implementing that research for obvious gains.

Rise of Cyberattacks/War on Ukraine

Cyber attacks are on the rise, the Ukraine War is an example of how cyber attacks will be used against other nations, in this case Russian backed cyber attacks are expected to become more prevalent. Russia declared war on Ukraine in early 2022, since that time America has provided the brave soldiers defending Ukraine with weapons and technology. In addition to sending equipment to aid the defending forces of Ukraine, the U.S. and its Allies have started levying sanctions against Russia. With those in mind experts have determined that more attacks will be carried out in cyber attack(s). A report laid out by European Union Agency for Cybersecurity Executive Juhan Lepassar has this to say "About 24% of cybersecurity attacks targeted public administration and governments while 13% targeted digital services providers, the report said." (Chee). Cyber attacks have become so prevalent that the Ukraine government is preparing for

massive cyber attacks by Russia; these attacks are likely[1] to involve denial of service attacks and target critical infrastructure, with an emphasis on Electricity.

Olympic Destroyer

The Olympics of 2018, in Pyeongchang, Korea, is a good example of how harmful cyber attacks can be. Before the opening ceremonies commenced, there was an attack on the cyber infrastructure of the Stadiums; this attack was able to knock out wifi access and keycards across the event. What ensued was a harried and tireless effort by the support staff of that event, who eventually were able to beat this cyber attack. What makes this a bigger event came about when they were deciding who did this attack, with evidence they found while fighting this threat, and the attackers wanted to make it unclear who was doing this. The software that was used in this attack was like a Chinese virus, with North Korea application style headers, and a Russian motive. Eventually it was determined that the Russians had made this software and then tried to make it look like it was from two different sources; this is huge, imagine a similar attack taking place on transformers, and a war is started with someone because the code was made to look like their handiwork. After multiple attempts to figure out who did this, Michael Matonis from FireEye (A cybersecurity company) figured out that it was Russia only because "Both hacks had used the same domain; account-loginserve.com…"[2] (Rhysider); this was in reference to the fact that the location the hack came from was the same as Russia used to carry out the alleged attack on our voting machines in 2016.

From the attacks on the Olympics to the rise in the threat of Cyber attacks in the wake of the attempted invasion of Ukraine, it is clear that we need to do something to protect our energy. This Bill and our Representative are both solutions to that problem. Armed with research and development, our great nation will triumph over all those who seek to cripple our energy infrastructure.

Sincerely,
Office of Tita Canduit.

[1] Denial of Service attacks are where you overload a cyber resource with requests, in order to overload and stop that resource from working.
[2] I would recommend you all listen to this podcast, Darknet Diaries, to understand the full scope of cyber warfare as it exists.

References:

1. H.R.5760 - 116th Congress (2019-2020): Grid Security Research and Development Act. (2020, September 30). https://www.congress.gov/bill/116th-congress/house-bill/5760
2. Chee F. Y. *Ukraine war, geopolitics fuelling cybersecurity attacks -EU agency.* (2022, November 3). Reuters. https://www.reuters.com/world/europe/ukraine-war-geopolitics-fuelling-cybersecurity-attacks-eu-agency-2022-11-03/
3. Pearson J. *West warns of Russian cyberattacks on critical infrastructure.* (2022, April 20). Reuters. https://www.reuters.com/world/europe/west-warns-russian-cyberattacks-critical-infrastructure-2022-04-20/
4. Kagubare I. *Ukraine warns of 'massive' Russian cyberattacks against critical infrastructure.* (2022, Sept. 27). The Hill. https://thehill.com/policy/cybersecurity/3663611-ukraine-warns-of-massive-russian-cyberattacks-against-critical-infrastructure/
5. Gambrell J. *Analysts: Fire at Iran nuclear site hit centrifuge facility.* (2022, July 2). AP News. https://apnews.com/article/50c3e7f6445ae99def6bdc65fbce6c42
6. Rhysider J. (Host). *Olympic Destroyer.* (2022). Darknet Diaries. https://darknetdiaries.com/transcript/77/
7. Bing C. and Satter R. *U.S. says advanced hackers have shown ability to hijack infrastructure.* (2022, April 14) Reuters Technology. https://www.reuters.com/technology/us-says-advanced-hackers-have-demonstrated-ability-hijack-multiple-industrial-2022-04-13/