MEMORANDUM

To: GuidePost Clients
From: GuidePost Strategies
RE: Securing Cyberspace: Business & the Economy
Date: October 19, 2022

OVERVIEW

On Wednesday, Oct. 19, **Rep. Jim Langevin (D-R.I.)**, co-chair of the Congressional Cybersecurity Caucus, and **Dmitri Alperovitch**, co-founder and chair of Silverado Policy Accelerator, joined **Washington Post Live** to assess how businesses can navigate the threat landscape, the impact on the national economy and ways to grow the cyber workforce. With the rise in ransomware attacks and data breaches, cybersecurity has surged in importance as a business and an economic issue.

KEY TAKEAWAYS

- The U.S. has entered a point where it is time to be cognizant about potential cybersecurity attacks from Russia. The U.S. needs to pay even more attention now that the infrastructure is at a vital state. Vladimir Putin is steadily increasing and instigating the conflict between the U.S. and Russia, and is behind some of the pipelines to Europe. This leaves an ominous sign they will directly attack U.S. infrastructure. Cybersecurity is likely to be the first weapon of defense.

- Since the war on Ukraine has begun, the U.S. has seen little to no action from Russia, surprisingly. However, we have entered a new stage where Putin realizes the war is not going in his favor and the U.S. needs to up the ante, especially after sanctioning off some goods and resources to Russia.

    - Russia is very well capable of pulling off an attack. Currently, the sanctions are crippling them globally. The most impactful measure the U.S. has implemented is the **Foreign Product Direct Rule** which is used as an export control measure. With that, Russia has had a difficult time importing chips.

    - Russia's capabilities on cyber still remain a threat and challenge. The U.S. has not seen a massive attack, possibly because U.S. involvement and support to Ukraine. With that said, it is important to not let that be a determining factor; and the U.S. has implemented programs that have shields in place for protection.

- The U.S. articulates a strong strategy for cyber-attacks. When it comes to dealing with Russia, the U.S. should not play the role of "tit-for-tat". Russia is capable and willing to do serious damage that goes beyond threatening cybersecurity. Instead, the U.S. should demonstrate the ability to conquer and overcome.

- There is a level of consensus when it comes to cyber norms but little to no consensus on the articulation front; and there needs to be an enforcement strategy in place. Calling out bad actors and demanding punishment is the appropriate process when they violate norms. The cyber norms in place should not involve attacking another country in peace. Supporting all efforts and building resiliency with partners and allies is key.

- When it comes to China, there are no longer conversations of attacks on intelligent independent companies. The U.S. is now looking into targeting the entire sector. This includes from the production to manufacturing to the workplace as relates to the semiconductor industry.

    - Semiconductors have a big impact on China. If the U.S. decides to move forward with an attack, many people will have to leave the industry at the risk of U.S. prosecution law. This serves as a declaration of economic war to achieve CHIP independence. There is no retaliation in the near time, but this can potentially change after the election.

- Russia, China, Iran, and North Korea pose the greatest cybersecurity threat. Their cyber capabilities are strong and could be used against the U.S. China, for example, uses cyber espionage that affects intellectual property rights (an area in which the U.S. needs to work harder).

- The U.S. needs to double down on vigilance. The **Cybersecurity and Infrastructure Security Agency (CISA)** is working closely with state governments to have resources in place. The integrity of elections is at stake, which is why vigilance plays an important role.

- A role for public and private partnerships needs to be encouraged with states and allies alike. State and local governments will never have the resources alone, but with the inclusion of Congress, the goals will be easily accomplished.

    - There also needs to be better partnerships within the industry. A joint collaborative effort is important to help mitigate threats. Sharing information and understanding that in context in real time is integral, especially when it comes to Secure Information Exchange (SIE).

- Congress has evolved mainly on awareness levels. The Cyber Security Commission, for example, has the ability to implement and change legislative activity to better alter decisions for the benefit of the nation. This is key when it comes to funding and growing CISA.

- The cybersecurity workforce gap is a growing challenge; simply put, the industry needs people. There can be more encouragement practices and incentives in place to combat this issue, such as the **Cyber Core Program**, a scholarship program which outlines a great example of incentive practices.

- Willingness, readiness, preparedness, and responsiveness are key when it comes to cyber security attacks from Russia and other countries. The U.S., with the leadership from the Administration, is at a premier spot now; the right strategies and the right people are in place.