CYBERCONFLICT STRATEGY

EVENT SUMMARY

OCTOBER

MODERATOR

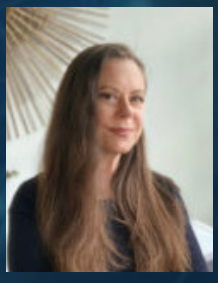
Dr. Michael Fritze
Vice President, the Potomac Institute for Policy Studies

PANELISTS

Melissa Hathaway
Member of the Board of Regents and Senior Fellow, the Potomac Institute; Senior Advisor, Harvard Kennedy School's Belfer Center for Science and International Affairs

Ari Schwartz
Managing Director of Cybersecurity Services, Venable

Richard Andres
Full Professor of National Security Strategy, National War College



Gentry Lane
CEO, ANOVA Intelligence Adjunct Fellow, PIPS, Visiting Fellow, National Security Institute at George Mason University's Antonin Scalia Law School

Image: pixabay/CoolVid-Shows

INTRODUCTION

In the cyber domain, the United States' borders are not protected by allies or oceans, allowing adversaries unprecedented proximity to the United States' critical infrastructure. Recent major cybersecurity events have clearly outlined the scope of the threats we face. The United States needs to prepare a whole-of-nation strategy to rebuff these threats in cyberspace. Though our adversaries are not coordinating their efforts, their combined efforts are force-multiplying each other's work.

According to our panelists, and experts throughout the field, the United States' critical infrastructure is extremely vulnerable to nation-state perpetuated cyber aggression. The companies themselves, as well as the chain of businesses which support them, are being breached daily. Many private and public companies responsible for American's most critical functions lack basic cybersecurity hygiene. Critical infrastructure are high-value targets, especially during wartime. What is different now is that the U.S.'s adversaries are going after these assets during peacetime. The escalating scope, scale, and impact of ransomware since the beginning of the pandemic have grown significantly, and reporting of these attacks has increased dramatically.

Based on the recent summit between President Biden and Vladimir Putin, this is only the beginning of the beginning, not the beginning of the end of cyber negotiations. According to General Nakasone, Commander of US Cyber Command, who said this during a public Congressional hearing, Russians have compromised electrical grid. Them pulling the trigger would be catastrophic. The United States must make a whole-of-nation effort to prepare for this ever-growing threat surface.

The Potomac Institute's esteemed panelists provided insights into the world of cybercriminality and warfare, considered the geopolitics of cyberspace, and offered their thoughts and recommendations as to how our nation can respond.

Image: pexels/Tima Miroshnichenkos

Image: pixabay/Tumisu

NATION STATES AS SAFE HARBORS FOR CRIMINALS

Criminals are safe from extradition. The idea that Russia, for example, is not perfectly aware of the cybercriminals that operate out of the country is naïve. The criminals, for their part, may be acting almost entirely out of desire for money, but the states that harbor them are getting something much more important: they are gaining an infrastructure of capable, skilled, and often trained individuals that can conduct sophisticated, and sometimes devastating, cyber operations. Though not conducted at the behest of adversarial governments, these criminal gangs run like a mafia-protected system in Russia.

The United States must develop a separate strategy for deterring foreign cybercriminals to halt further. For example, cybercriminals took down the health system in Ireland, and that attack directly caused deaths in that country. Similar, and potentially worse attacks than that have already occurred in the United States. The United States government would be naïve to assume that it will not happen again. The United States government needs to make it clear that countries that harbor cybercriminals will face consequences.

According to one of the panelists, a potential course of action would be to designate these cybercriminals as terrorists. That would provide the administration important tools to take down these networks through extra-territorial actions. Some experts believe that the United States, in accordance with the Law of Armed Conflict, in the name of self-defense, could go into foreign territory and break up cybercriminal networks. The United States needs to rely on its allies in creating an international understanding that conducting what is effectively state-sponsored cyber-terrorism is unacceptable.

Image: Shutterstock/LukeOnTheRoad

NOTABLE ADVERSARIES

RUSSIA

To understand Russia, one must look at the larger geopolitical picture. President Putin has found innovative ways to exert influence through cyberspace regardless of their comparative conventional military disadvantage. One of our panelists believes that their goal is to bring cyber weapons into the arms control regime and to be recognized as a major global player, especially in the eyes of eastern European states as the European Union weakens.

The Russian government has made concessions to the United States, saying that they would crack down on cyber gangs within their country. Our experts agree that Putin and his administration are well aware of the cybercriminal activity taking place within their borders. This is likely an empty gesture, and the United States should operate under the assumption that attacks from this region will continue.

CHINA

For years, the Chinese goals in cyberspace focused intellectual property theft, industrial espionage and collecting as much personal identifying information on as many people around the world as they could.

The Chinese endeavor to control the very infrastructure and technology that forms the foundation of the internet. They've doubled down on efforts to control 5G networks, the microelectronics that we use in our systems, and access points around the world. This is a growing concern that will need to be addressed.

RECOMMENDATIONS

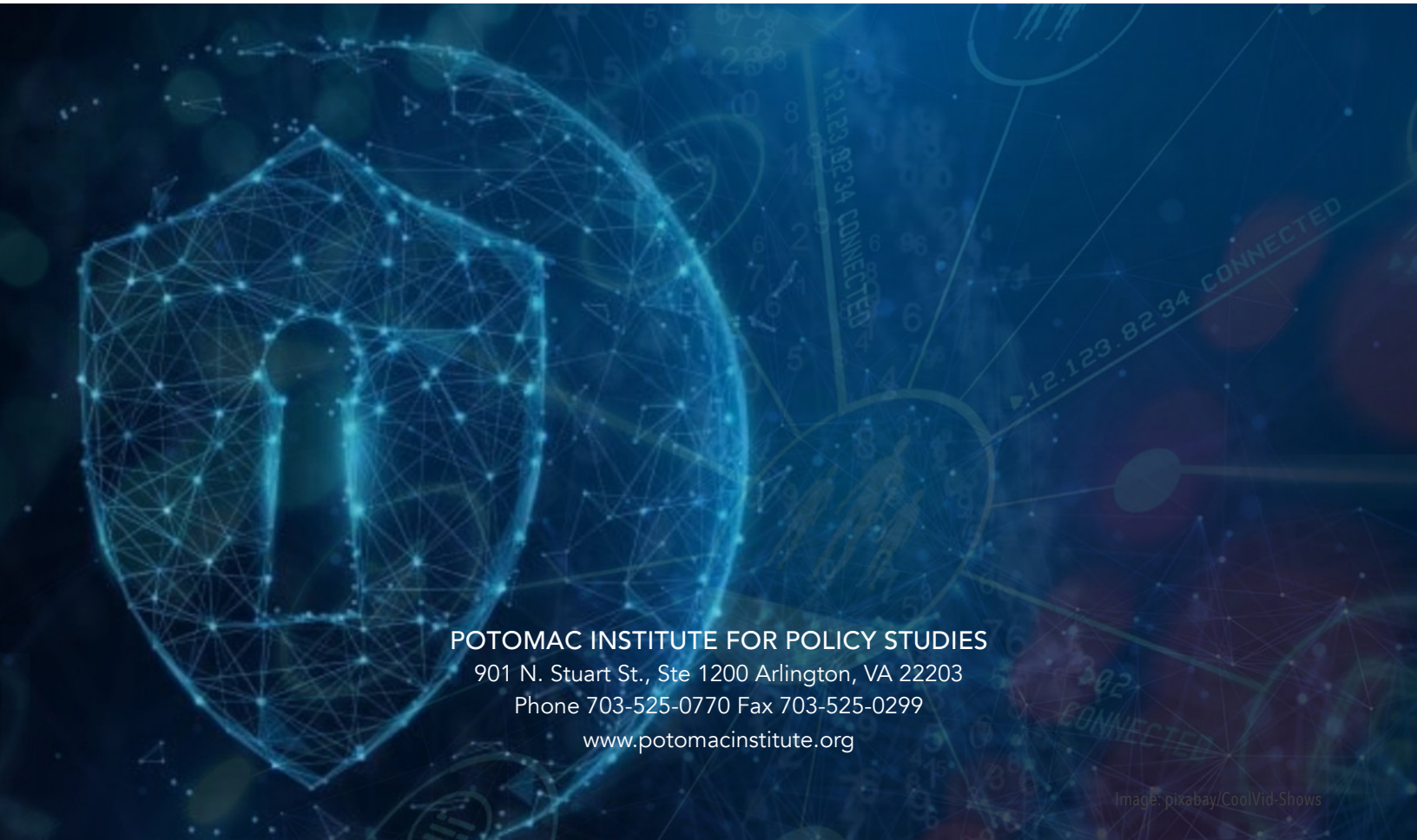
One of the panelists argued that efforts to navigate this era of cyber warfare need to be led by the White House. The Executive Order from May of 2021 made significant progress in establishing standards for government agencies. However, this is not enough to protect our largely privatized critical infrastructure.

As cybersecurity events continue to threaten critical infrastructure in the United States, the whole nation needs to have a concerted strategy. Cyber threats should be no exception. There are many avenues by which the United States can impose consequences to those countries harboring cybercriminals. The difficult question to answer, however, is what is the proportional response?

Most of our critical infrastructure – 85% of it – is in the hands of the civilian sector. Congress must produce legislation that can effectively incentivize companies to make the necessary investments to insulate themselves and their customers from harm driven by gaps in cybersecurity. The government, for the sake of the public good, must ensure this level of security.

CONCLUSION

The United States faces an unprecedented threat in cyberspace. Every adversary should be taken seriously. Our infrastructures have such true vulnerabilities at the cores of every system that it is relatively inexpensive and easy to cause harm. With that in mind, we should not focus all of our efforts on one single threat. A unified strategy that can handle the growing threat of cybercriminals as well as the growing list of nation-state actors is an imperative that must be met.



POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St., Ste 1200 Arlington, VA 22203
Phone 703-525-0770 Fax 703-525-0299
www.potomacinstitute.org

Image: pixabay/CoolVid-Shows