The Role of Cyber Threat in the International Relations and Affairs Arena: Understanding the Sensitivity of Access, Attribution, and Intent of The Cyber Actor.

Andres G. Alvarez

Florida International University

ISS3613: Issues in global Cybersecurity policy

Prof. Robert Boyd

July 3, 2021

The Role of Cyber Threat in the International Relations and Affairs Arena

Progress in technology has given birth to computer networks, giving our world unprecedented access to share information in seconds without much importance on the distances at play to relay such messages. These networks have dramatically changed how we conduct our lives, but it has also had significant implications for security, diplomacy, and international relations. This new rise in connected networks, known as the cyberspace domain, is an opportunity to influence power distribution. The cyberspace domain has left many states with chances to increase their influence. Still, it has also increased their vulnerabilities and left states with many attack vectors. Nations such as Russia, China, Iran, North Korea, or other non-state actors exploit those vulnerabilities by attacking new vectors. Dr. Adam Cobb said, "After land, sea, air, and space, warfare has entered the fifth domain: cyberspace" (Cobb, A, 2004).

Due to the rise of the digital age, information has become more centralized, allowing for potentially more harmful insider attacks with actors with access to essential assets, databases, and Programs, creating more conflicting international relationships similar to what happened with the Snowden incident. Russia and China refused any extradition attempts for the opportunity they had to damage the image of the U.S. Russia ended up giving temporary asylum to Snowden. To this day, he is granted asylum by them. The Snowden story was received with great admiration by U.S. rivals like Putin, who tried to twist the story in Russia's favor by saying, "Trying to spy on your allies, if you consider them allies and not vassals, is just indecent. It undermines trust, and in the end, damage your national security." (Osborn, A, 2017). China's CCP also had some

similar comments praising the actions of the so-called young activists, saying, "fearlessness that tore off Washington's sanctimonious mask" (Gray, D, 2013). Brazil's president, Dilma Rousseff, also reacted by canceling her visits indefinitely to the U.S. due to the Snowden scandal. These examples show how simple cyberspace and international relations are to fuse into one big problem or how one affects the other; we have entered a new age of states conducting surveillance through cyberspace.

In late 2020 and the beginning of the year 2021, the Orion SolarWinds attack happened. The SolarWinds attack clearly delineates how intertwined cyberspace and international relations are. The attack targeted a large and reputable U.S. Cybersecurity company; as of the attacks, the company's products were being used by more than 300,000 customers worldwide. They range from organizations/companies such as the Pentagon, NASA, NSA, State Department, Office of the President, Microsoft, and many other big names. The attack is believed to be a State-sponsored incident where the Russians built a collaborative effort with cyber experts to penetrate the company's security products to harvest information and state that their capabilities in the cyber realm are to be considered a real threat (Tran, C, 2021). Although 80% of the attack focused on customers in the U.S., it also identified victims in several countries. It includes Canada and Mexico in North America; Belgium, Spain, and the U.K. in Europe; Israel and the UAE. The only certainty of this attack is that the number of victims will continue to expand (Smith, B., 2021).

After seeing the large number of attacks and methods that the cyber threat represents, there is a clear future vision. The number of attacks will continue to grow and

increase in penetration capabilities. Some patterns emerge from past experiences. In examples where insiders reveal secret information, there is a solid commitment to protect such actors from those nations who can benefit from the leak. Power projection and capabilities have always been in play in international relations, and states will continue to look for ways to balance this in their favor. Cyberspace offers a unique opportunity for States and even Non-state actors to swing the balance of power in the way they think is appropriate. Cyber-attacks provide offensive capabilities for malicious actors with a degree to cloak their attacks in a challenging time, pinpointing the exact source or perpetrator of the episode without making some assumptions and building up the evidence for each case. There should be a sense of urgency in the policy realm to address this cyber threat issue and how it can relate to or affect international relations between states. The growing capabilities will continue to enable states and non-state actors to launch attacks against critical infrastructure and other critical sectors vital to a State; causing damage or exfiltrating information can tip the balance of power as they see fit.

Someone must explore the relationship between cyber and international relations in a more collaborative and open-minded effort. Private and public sectors should combine their knowledge and capabilities to tackle this issue to provide a more precise and safe way to recover and prevent cyberattacks while minimizing them. For policymakers to make cyber-attacks less effective in altering international relations, policymakers must invest in funding the capabilities of their industry to make way for new studies, defensive and offensive capabilities, and responses to such incidents. There is a need for accountability in the intertwined cyberspace and international relations until

new policies and innovative ways of thinking; the lingering menace of a cyber-attack breaking the entire global system will continue to exist.

For the world to approach cyber-attacks, we must change our current approach to the ever-evolving problem. There is also the need for a more effective strategy and understanding of entering the future ahead. First, the continuing rise in the determination and capabilities of nation-state attacks will grow. Second, the world needs a more effective strategy to protect and recover against cyber-attacks. Third, there is a need to take a significant step into sharing and analyzing threat intelligence. Fourth, strengthen international rules to put reckless nation-state behavior out of bounds and ensure domestic laws keep pace with the rise of the cyber threat. Fifth and final, we need some form to attach accountability for cyberattacks.

We have seen that policymakers struggle to understand the complexities of cyberspace, limiting their ability to issue strong legislation that would potentially benefit the intersection between Cyber and International relations. Policymakers need to understand the effects and risks that acting in the cyber world can cause; there must be a consensus on cybersecurity for those in charge of the laws before committing to any new policies or regulations. The cyber threat issue must be approached with an international collaborative effort; collaboration is vital to growing the base knowledge. It will lead to better-crafted laws on a global level, limiting the impact potential Cyber threats can have on influencing International Relations with allies and enemies.

Much of the effort to be done in the future involves higher thought of methods, empirics, evidence, and critical thinking approaches that would test the nature of institutional provisions regarding cyberspace. The moral boundaries of cyber seem clear

but are not a guarantee, given the latent harm to citizens. The world needs more considerable care in indicating cyberspace's strategic rules and opportunities. Developing policy areas need not be jam-packed with reactionary policies. No scholar, politician, or Engineer can tackle the great majority of Cyber issues with one approach; it needs to be packed out and examined individually. The world needs to reflect that the Cyber field frequently needs reset and monitoring, given its importance. Due to the standing of research in the Cyber field, arrangements in the domain bring superior risks and tremendous potential. Cyber will continue to disturb the present and future state of International Relations. Without any accountability, the issue will continue to evolve and rise; the global effort for accountability in cyber needs to be considered a means to protect the current and future stability. It is difficult for the cyber industry and the collective security of international relations, but nothing creativity, collaboration, and innovation can not achieve. The world’s Cyber and International Relations future is walking a fine line between solidity and anarchy. Still, the reflection that cooperation presently leads the space should be encouraging to some degree.

References

Cobb, A. (2004, February 24). Warning on cyber terror. The Sydney Morning Herald. https://www.smh.com.au/technology/warning-on-cyber-terror-20040224-gdiev7.html.

Osborn, A. (2017, June 2). Putin says Snowden was wrong to leak secrets but is no traitor. Reuters. https://www.reuters.com/article/us-russia-putin-snowden-idUSKBN18T1T4.

Gray, D. (2013, June 25). 'Mad invader, eavesdropper': China slams U.S. after Snowden accusations. R.T. International. https://www.rt.com/news/china-rights-snowden-us-194/.

Tran, C. (2021, June 17). The SolarWinds Attack and Its Lessons. E. https://www.e-ir.info/2021/06/17/the-solarwinds-attack-and-its-lessons/.

Smith, B. (2021, June 15). A moment of reckoning: the need for a strong global cybersecurity response. Microsoft On the Issues. https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/.