Proactive Cyber Policies Are Needed

Jiachen Liu

Abstract

The anarchic nature of cyberspace makes it difficult to effectively control cyber attacks targeting civilians and even national facilities. This uncontrollable and potentially explosive danger must be immediately contained from realists' perspective. In addition, weaponized cyber attacks can also become a means for hostile forces to weaken the strength of other countries, posing an imminent threat to the country's survival. Given the invisible nature of cyber attacks, a country should have policies and means to proactively detect and destroy potential cyber threats.

Keywords: Cyber attacks, realism, proactive policies

Introduction

In recent years, cyber operations have become more and more widely used as a means of obtaining intelligence remotely. Under the leadership of the United States, G7 countries have begun to proactively inspect their communication infrastructure for devices manufactured by countries that are ideologically opposed to them. In September, Asian media also broke the news that a spyware called Suctionchar has been exposed to be involved in attacks against universities associated with the militaries1. In addition, most widely known, cyber operations are used for sabotage military purposes in war zones in East Europe. These have further deepened the impression of cyber attacks in people's minds.

Liberal assessments of cyber action have been primarily negative. These people believe that international actors are not only states but also international organizations, companies, and individuals. They advocate international norms and cooperation to maintain the world order, and cyber operations will weaken the cooperation intentions among international actors. However, from a realist point of view, cyber operations are necessary. All significant powers should maintain investment and development in cyberspace and adopt a more active cyber policy externally. This article will illustrate this point by explaining the threat posed by irrational people on the Internet, the social impact of cybercriminal activity, and the need for pre-emptive action.

Invisible threats against the public

First of all, cyberspace is anarchy, which is the same world order in the eyes of realists. Cyberspace also lacks norms that are commonly recognized as in reality. John Perry Barlow's 1996 Declaration of the Independence of Cyberspace states that the Internet space should remain free from government regulation2, which is precisely what cyber-sovereignty means: independence from the sovereignty of individual countries and thus free from interference. Based on this, the theory of "Popular Sovereignty in Cyberspace"3 points out that the netizens active in cyberspace hold the sovereignty of this space, not the government entities. This also means that every active user in cyberspace has discretionary power simultaneously. It may be a good thing for liberals that cyberspace is free from political oppression. But is this a good thing in reality? Cyberspace users are not like actors in the real world and are not all rational actors. Because of the easy accessibility of the web, no one can predict whether users living in this space will cause harm to others.

Earthweb's 2022 statistics show that 6% of total web traffic goes to the dark web, with only 22.6% of activities in the non-illegal category. In addition to accounting for 8.1% of drug sales and 6.3% of illicit financing, dark web users demand three times more malware than supply, making it one of the most popular illegal online activities4. Due to the anonymity of the Onion service and the newer encryption system, the dark web provides these evils with untraceability and better concealment5. Coupled with the special sovereignty of cyberspace activities, there is a lack of real-time supervision and control of "crimes" like law enforcement. We can never predict and completely eradicate malicious behavior in cyberspace. According to FBI investigators, the identity information of every American citizen can be easily obtained on the dark web. In the face of such a stark reality, we should do something about it. Anarchic cyberspace is rife with criminal activity against the populace, and the sources of these challenges are often untraceable and ineradicable, originating from all over the world. From a realist perspective, we should improve existing policies on cyberspace and strengthen the management and control of these existing risks to not cause social instability.

Weaponized means against sovereignties

In addition to the impact of civil malicious behavior on cyberspace security, we should also take precautions against cyber threats issued by organized and premeditated state agencies because their effect is often more severe and broader. At the end of 2020, SolarWinds, which hackers implanted into Trojan horses, caused the network of several USUS federal government agencies to be intruded on, including not only civilian departments such as the Department of Treasury and the National Telecommunications and Information Administration but also sensitive military-related-departments such as the Department of Defense and the Nuclear Security Agency7.

By analyzing the stolen data, the initiator of the attack may have gained access to multiple state secrets, including the flow of government funds, citizens' communications, and even information about the nuclear industry, which severely weakens USUS capabilities. In this way, the country that initiates the cyber attack can have relative gain, thereby increasing their country's power in the world. In realist theory, this phenomenon is seen as a threat to the country's survival. We also need more aggressive and pre-emptive cyber means to maintain the balance of power in anarchy to ensure our survival. However, because of the anonymity of the Internet, it is often difficult to distinguish these organized state behaviors from private ones. Therefore, we should positively respond to cyber attacks without demarcation and thwart all attacks, whether civil crimes or state actions.

A well-known secret

Of course, a more radical and pre-emptive approach could be criticized by realists for undermining trust in international cooperation. While these measures will adversely affect the flow of the economy and the development of global supply chains, they will have little impact on the political and military relationship between us and our allies. After the PRISM program was exposed, NATO members responded mostly to verbal criticism, establishment of bills, and escalation of domestic cyber defense systems, with no substantive diplomatic or military response to the United States8. Germany and Japan have even begun to develop their network monitoring methods, and the international community seems to have acquiesced in the necessity and legitimacy of monitoring.

Policies suggested

Proactive cyber policies should include the following means to deal with the growing cyber threats.

1. The first is continuous monitoring and risk assessment. At the same time, to improve defense efficiency, the main objects of monitoring and evaluation should be selected to be national facilities and large domestic companies involving the interests of many populations. This behavior aims to search for security risks in the domestic network and block any threats, including Trojan Horses and back door programs.

2. Secondly, given the invisible nature of network security risks, we must actively search for attack intentions in domestic and foreign networks. The search method for attack intent here is not limited to infiltrating domestic and foreign hacker alliances and intelligence organization networks by organizing network technicians. Still, it should also pay attention to current trends and strengthen attention to network fluctuations in related fields. The PRISM project mentioned above would be the best example.

3. Finally, cyber warfare has become a new mode of warfare. And like all other wars, security dilemmas are also inevitable. We cannot guarantee that the new weapons developed by our opponents will not pose a threat to us. Therefore, as a means of checks and balances, we must study equivalent or even higher-level cyber weapons to ensure the "mutual destruction" in cyber warfare. And, after the network attacks our side, we should not hesitate to retaliate in a way that is no lower than the level of attack launched by the other party to prove our side's determination and capability that would deter opponents from initiating next strikes.

Conclusion

To sum up, cyber operations are a crucial item we should focus on now, and we need more proactive, pre-emptive cyber foreign policy. The Defend Forward strategy proposed by Paul C. Ney, general counsel of DoD, is a good idea. By establishing a cyber force to proactively search for and thwart an adversary's cyber conspiracy9, the harm done by the irrational actors, the blatant crimes in cyberspace, and the balance of power under the cyber anarchy can be well addressed at the same time.

Reference

1. 王 怡 . (2022, September 12). 西工大被美国网络攻击又一重要细节曝光！要小心”饮茶”！ . 环球网 . Retrieved November 19, 2022, from https://world.huanqiu.com/article/49dPkUR2N0C

2. Barlow, J. P. (1996). Declaration of independence for cyberspace. *RhetNet: A Dialogic Publishing (Ad)Venture.* https://doi.org/10.37514/rnt-j.1996.3.6.21

3. Mueller M (2017) *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace. Malden,* MA: Polity.

4. Georgiev, D. (2022, November 10). *How much of the Internet is the dark web in 2022?* Techjury. Retrieved November 19, 2022, from https://techjury.net/blog/how-much-of-theinternet-is-the-dark-web/#gref

5. Greenberg, A. (2017, January 20). *The darknet is evolving to offer more secrecy than ever.* Wired. Retrieved November 19, 2022, from https://www.wired.com/2017/01/get-even-easierhide-dark-web/

6. Journal, E. P. T. W. S. (2018, December 14). *Thieves can now Nab your data in a few minutes for a few Bucks.* The Wall Street Journal. Retrieved November 19, 2022, from https://www.wsj.com/articles/what-happens-to-your-data-after-a-hack-1544367600? mod=hp_lead_pos10

7. Saheed Oladimeji, S. M. K. (2022, June 29). *Solarwinds Hack explained Everything you need to know.* WhatIs.com. Retrieved November 19, 2022, from https://www.techtarget.com/ whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

8. Essers, L. (2014). *Merkel and Hollande to talk about avoiding USUS servers.* ITworld. Retrieved November 19, 2022, from https://web.archive.org/web/20140221104005/http:// www.itworld.com/security/405353/merkel-and-Hollande-talk-about-avoiding-us-servers

9. Jensen, E. T. (2020, October 21). *Due diligence and the USUS defend forward cyber strategy.* Lawfare. Retrieved November 19, 2022, from https://www.lawfareblog.com/due-diligenceand-us-defend-forward-cyber-strategy