Jonah Feldman

Ming Chow

COMP-116

6 December 2017

The Internet's Security Dilemma: Why Cyber-Weapons Beget Instability

Abstract

This paper analyzes interstate cyberwarfare through the lens of Robert Jervis's offense/defense paradigm. In this paradigm, two factors are important in determining technology's impact on global stability: whether a technology favors offensive or defensive strategy, and whether offensive technology can be distinguished from defensive technology. This paper argues that cybersecurity exemplifies Jervis's "third world," where offense has the advantage while offensive and defensive technologies are easily distinguishable. The case for offense/defense distinguishability is straightforward: defensive tactics like encryption, firewalls, and air gapping have little offensive utility. Thus, this paper will focus primarily on cybersecurity's offensive advantages and its implications for the international system.

In Jervis's "third world," cooperation is still possible among status-quo states because they can pursue defensive strategies that do not engender the security dilemma. However, this paper argues the rapid proliferation of information technology among small and medium powers will greatly enhance the odds of cyberwarfare spiraling into interstate conflict. This paper also suggests legal and regulatory strategies states can undertake to increase the value of cyber defense and therefore decrease the risk of cyberwarfare.

Introduction

From the rifled musket to the intercontinental ballistic missile, advances in technology have constantly reshaped the face of warfare. Beyond giving a tactical edge to technologically advanced nations, technology has often altered the structural incentives of states and upended previous balances of power. The increasing proliferation of cyber conflict and cyber-weapons presaged by the rise of the internet has left policymakers scrambling for answers on what these new technologies mean for international politics

Perhaps the most rigorous framework for analyzing technology's impact on international relations remains Robert Jervis's offense/defense paradigm.[1] Jervis's framework poses two questions: Does new technology favor offensive or defensive tactics, and can offensive technology be easily distinguished from defensive technology? Defensive technology is defined as technology that raises the security of a given state without significantly decreasing the security of its neighbors, whereas offensive technology necessitates a decrease in neighboring states security. Permutations of those two variables form four possible worlds, each with varying incentives and degrees of instability.

This paper argues that cyber-weapons fall into the third of these four worlds; cyber offense is easily distinguishable from cyber defense, but cyber-weapons favor offense over defense. While Jervis believes[2] that peace is still possible in this scenario, this paper argues that the rapid proliferation of cyber-weapons in addition to murky legal norms surrounding cyber conflict will result in increased risk of cyber-war and create a more unstable world.

[1] Jervis, Robert "Cooperation under the Security Dilemma." *World Politics*, Vol. 30, No.2, January 1978, pp 186
[2] Jervis, *Ibid*¸ pp. 213

To the Community

From both a computer science and international relations perspective, writing on cyber conflict has tended to focus on technical aspects of intrusion or on specific case studies. While such work is valuable, this paper intends to create a broader theoretical framework through which to analyze the international relations of cyberspace. Additionally, bridging the policy-technical divide remains one of the most vexing problems in computer security, and this paper attempts to present a mutually intelligible framework for understanding emerging technologies and their geopolitical impact. Both developers and policymakers would benefit from viewing emerging developments in computer security through the lens of the offense/defense paradigm. For developers, the paradigm should inform them how to design technology that incentivizes defense on a macro-level. For policymakers, the paradigm should help them understand state's reactions to cyber incidents and design policies to soften the instability begot by cyber-weapons.

Offense and Defense in Cyberspace

Few cyber-intrusion methods have applicability for cyber defense, and vice versa. Offensive tools that routinely make the OWASP top 10[3] like SQL Injection, Cross Site-Scripting, and Cross Site Request Forgery have little utility for defensive operations. Their fundamental structure is designed to destabilize and degrade the integrity of networks, the exact opposite of what cyber defense is intended to do. Unlike a gun or an artillery shell, SQL injections have very little ability to stop an attack that is underway. Conversely, defensive measures like encryption and two-factor authentication are not primarily offensive weapons. Even if ransomware like WannaCry uses encryption to ransom data,[4] it is a supplemental tool

[3] OWASP. "Category:OWASP Top Ten Project." *Category:OWASP Top Ten Project - OWASP*, 2017,
[4] Mercer, Christina. "How Does the Ransomware That Infected the NHS Actually Work?" *Techworld*, 15 May 2017

that can be used only after successful offensive intrusion, making it of tertiary importance at best to offensive operations

Critics of this viewpoint[5] argue that the technical skills required for both white and black hat hackers are similar, blurring the line between offense and defense. While this analysis has merit, it ignores the fundamentals of the security dilemma. States can proliferate advanced encryption algorithms or strengthen login credentials to critical databases without triggering fear or insecurity in other states. Air gapping the computer system for a dam would not trigger the same alarm that research into overriding dam controls would, and states can clearly delineate between the two.

Turning to the second variable in the security dilemma, the small economic and strategic cost of cyber offense relative to cyber defense gives offense a decisive advantage. The lack of deterrence in the realm of cyberwarfare increases the advantages of offense by lowering the expected retaliatory costs of attacks. Determining that an attack has taken place is often difficult and time-consuming process;[6] the "dwell time" before administrators realize a system has been compromised often runs into months. An attack on physical infrastructure like a dam or an electric grid might be attributed to deteriorating physical conditions well before someone suspects foreign intrusion into computer control systems, and malware that steals sensitive information may go undetected indefinitely. Even after an attack has been identified, discovering the identity of the perpetrating state or organization is extremely difficult. It is notoriously difficult[7] to technically trace the source of a cyberattack, as identifying metadata can be easily spoofed. Furthermore, attacks are often carried out by "patriotic hackers" with murky links to the

[5] Farrell, Henry. "Distinguishing Offense from Defense in Cybersecurity." *The Monkey Cage*, 5 July 2013
[6] Unver, H Akin. "Do Trees Fall in Cyberspace?" *War on the Rocks*, 8 Dec. 2017
[7] Newman, Lily Hay. "Why Is It So Hard to Prove Russia Hacked the DNC?" *Wired*, Conde Nast, 3 June 2017

states that may or may not be sponsoring them, making it difficult to credibly blame a state for an attack. With these obstacles to retaliating against a cyberattack, states feel less of a political cost to invest in and carry out offensive operations against adversaries.

Furthermore, investing in cyber-offensive capabilities is relatively cheap. The price of processing power continues to drop at a rate of tenfold every four years[8], making investment in physical infrastructure needed to carry out attacks extremely low. Although investing in human capital can be relatively expensive, the cost is mitigated by the fact that the both the "dark web" and normal internet are already littered with ready-to-go attack tools intended to penetrate and/or degrade foreign networks. Cyber-weapons are already out there at an extremely low cost;[9] states merely need to reach out and take them.

By contrast, the cost of defense is structurally high and rises exponentially. For every line of additional code written, the complexity of programs rises exponentially, and thus the number of potential bugs and vulnerabilities likewise rise exponentially. The problem is compounded by the fact that a defender must protect against every possible venue of intrusion, whereas an attacker only needs to find a single flaw in order to gain access to or degrade a system. Furthermore, economic incentives will make nationally critical economic sectors reluctant to undertake good cybersecurity practices.[10] Although it may be safer for national security reasons for the electrical grid to be air-gapped from any network, the relative economic cost of being disconnected from real-time data on electricity usage will push companies to increase their own vulnerability to cyber-attacks. This is especially true in completive industries where firms can be

[8] AI Timelines. "Trends in the Cost of Computing." *AI Impacts*
[9] Lynn, William J. "Defending a New Domain." *Foreign Affairs*, Council on Foreign Relations, 30 May 2014
[10] Serena, Chad C. and Colin P. Clarke. "America's Cyber Security Dilemma - and A Way Out." *Defense One*, 22 Dec. 2016

bankrupted for failing to keep up with their networking opposition. The same incentive holds true in military technology; states will be reluctant to handicap battlefield tactical advantages to protect against as yet theoretical security flaws, creating an opening for attackers to degrade or control the advanced military technology of developed states.[11] In software development, the logic of economic competition has already severely degraded the internet's collective security; race to the bottom incentives have caused companies to continually push out new software before it has been fully vetted and to later patch the software's numerous problems later, creating a hodgepodge of insecure partially updated software[12] that makes the internet collectively insecure and heightens the advantage of offense.

Consequences of an Offensive World

Offense has the advantage in emerging computer technologies and is distinguishable from defense; what are the international security implications? For the general offense/defense paradigm, Jervis argues that cooperation is still possible because status-quo states can successfully signal their peaceful intentions and cooperate to contain the ambitions of revisionist states.[13] However, this paper argues the severe imbalance of cost between offense and defense in cyberwarfare will raise tensions, spur arms races, and heighten instability, supercharging incentives for a first strike.

The low cost of cyber offense will likely lead medium sized and/or emerging powers to proliferate weapons as the cheapest way to make up for their conventional military deficiencies. This can already be observed as Russia and Iran invest in their cyber capabilities as a way to

[11] Lynn, *Ibid*
[12] Timberg, Craig. "These Hackers Warned the Internet Would Become a Security Disaster. Nobody Listened." *The Washington Post*, WP Company
[13] Jervis, *Ibid*, pp. 212

counter their conventional military disadvantage with Western-aligned powers.[14] With few legal or normative barriers to the acquisition of cyber-weapons, newly modernizing countries will likely see investing in intrusion methods as a cheap way to gain the advantage against regional rivals. The beginnings of this process have already begun in the Persian Gulf; the outbreak of the 2017 diplomatic crisis between the GCC and Qatar was preceded and followed by several UAE-sponsored hacks intended to degrade the Qatar-funded Al-Jazeera news station as well as frame Qatar as an ally of Iran.[15] Seeing rivals investing in offensive cyber capability and realizing the large cost of cyber defense, the only way states will be able to successfully militarily compete with their neighbors is to similarly invest in offensive capability. Coupled with the difficulty in predicting a cyber-attack,[16] spiraling arms races will give an overwhelming advantage to a first strike to cripple an enemy's offensive capability before they can use it, creating unstable conditions and mistrust between states.

The likelihood of conflict is also amplified due to cyberwarfare's interaction with Kenneth Waltz's lone predator theory. According to this theory, cooperation is difficult and conflict endemic to the international system because just one predatory state forces all other states to arm themselves and adopt militaristic attitudes to defend themselves.[17] The mere threat of one predatory state in an international system of hundreds of peaceful states will spur states to proliferate advanced weaponry. Jervis argues that when offense is distinct from defense, as is the case in the cyberwarfare, states can successfully signal their non-aggressive intentions.[18] This will lead to peaceful cooperation in geographic areas occupied by status-quo states. However, in

[14] Serena and Clarke, *Ibid*
[15] DeYoung, Karen, and Ellen Nakashima. "UAE Orchestrated Hacking of Qatari Government Sites, Sparking Regional Upheaval, According to U.S. Intelligence Officials." *The Washington Post*, WP Company, 16 July 2017
[16] Lynn, *Ibid*
[17] Waltz, Kenneth *Man, the State, and War,* New York: Columbia University Press, 1959, p. 232
[18] Jervis, *Ibid*, 210

a world full of cyber-weapons, states do not only have to worry about the aggressive intent of their neighbors, but also of *every single* other state that exists. And unlike other weapons that can be operated across large distances like ICMBs, cyber-weapons are cheap and can easily be acquired by almost all nations. The heightened state of insecurity will force states to counter in the only cost-efficient way possible (offense), ruining chances for cooperation among status-quo states by preventing them from signaling their peaceful intentions.

The final destabilizing aspect of cybersecurity is the attribution problem and the cloudy political norms surrounding cyberattacks. As discussed above, the difficulty in tracing the source of cyberattacks lowers the value of deterrence, removing restraints on states taking offensive action. Furthermore, states may rely too heavily on the attribution problem to obfuscate their attacks, and therefore accidentally trigger interstate conflict by conducting an aggressive attack they incorrectly assumed could not be traced back to them. The problem is compounded by the lack of international legal agreements and norms delineating espionage from acts of war in cyberspace. Does knocking out the banking websites of private firms count as an act of war? What about merely stealing analytical data from them? States may have differing conceptions as to what constitutes an act of war, triggering conflict when one state carries out what it thought was merely espionage while the victim state considers it an act of war. As new states continue to proliferate cyber-weapons, their inexperience will likely lead them to test out new weaponry and blunder into war.

Action Items

Unfortunately, the conditions shaping the persistent advantage of offense are baked into the structural technological and economic model of the internet, making it difficult to take action to limit the security dilemma. Besides praying for a technological breakthrough that will

fundamentally alter the comparative strength of offense and defense, there are two primary policies this paper recommends governments undertake to lower the risk of conflict.

First, governments can legislate domestic policies that encourage better security practices from corporations. Punishing corporations that push out sloppy software that requires constant updates while rewarding those that produce secure software would help improve the overall security of the internet. Governments could also require that devices that have not downloaded critical software updates be unable to connect to the internet until they are updated. In addition to beefing up overall security, such steps would also prevent attackers from creating botnets by harnessing the power of swathes of insecure devices, removing another tool from the attacker's arsenal. This would lessen the imbalance between offense and defense, reducing the expected gains to offense and lowering instability.

Second, governments should work internationally to codify laws surrounding the use of force in cyberspace. While there has been progress in the academic world delineating acts of war from regular day-to-day espionage,[19] legal and political progress has largely stalled. Clarification would prevent states from unintentionally engaging in overly aggressive actions that could trigger war. Additionally, such laws could provide dispute resolution mechanisms to deal with inevitable political conflicts in cyberspace, preventing states from resorting to war.

Conclusion

By giving states access to a cheap arsenal of technology that overwhelmingly favors offense, computers and networks are set to make international politics a more dangerous place.

[19] Desombre, Winnona. "Getting Harder to Catch: Analyzing the Evolution of China's Cyber Espionage Campaigns against the United States through a Case Study of APT1." *Sigma Iota Rho's Journal of International Relations*, vol. 19, 2017, pp. 85–87

Smaller and emerging states will see it as the easiest way to increase their military heft, and itchy trigger fingers and justifiable disregard for retaliation will make them eager to take actions that could lead their country into war. Although steps can be taken to soften the worst aspects of this new paradigm, for the most part the world is stuck with this new perilous balance of power.

Citations:

AI Timelines. “Trends in the Cost of Computing.” *AI Impacts*

Desombre, Winnona. “Getting Harder to Catch: Analyzing the Evolution of China’s Cyber Espionage Campaigns against the United States through a Case Study of APT1.” *Sigma Iota Rho's Journal of International Relations*, vol. 19, 2017, pp. 85–87

DeYoung, Karen, and Ellen Nakashima. “UAE Orchestrated Hacking of Qatari Government Sites, Sparking Regional Upheaval, According to U.S. Intelligence Officials.” *The Washington Post*, WP Company, 16 July 2017

Farrell, Henry. “Distinguishing Offense from Defense in Cybersecurity.” *The Monkey Cage*, 5 July 2013

Jervis, Robert “Cooperation under the Security Dilemma.” *World Politics*, Vol. 30, No.2, January 1978

Lynn, William J. “Defending a New Domain.” *Foreign Affairs*, Council on Foreign Relations, 30 May 2014

Mercer, Christina. “How Does the Ransomware That Infected the NHS Actually Work?” *Techworld*, 15 May 2017

Newman, Lily Hay. “Why Is It So Hard to Prove Russia Hacked the DNC?” *Wired*, Conde Nast, 3 June 2017

OWASP. “Category:OWASP Top Ten Project.” *Category:OWASP Top Ten Project - OWASP*, 2017

Serena, Chad C. and Colin P. Clarke. “America's Cyber Security Dilemma - and A Way Out.” *Defense One*, 22 Dec. 2016

Timberg, Craig. “These Hackers Warned the Internet Would Become a Security Disaster. Nobody Listened.” *The Washington Post*, WP Company

Unver, H Akin. “Do Trees Fall in Cyberspace?” *War on the Rocks*, 8 Dec. 2017

Waltz, Kenneth, *Man, the State, and War,* New York: Columbia University Press, 1959