CYBERSPACE AND NATIONAL SECURITY

CYBERSPACE AND NATIONAL SECURITY

Threats, Opportunities, and Power in a Virtual World

DEREK S. REVERON
Editor

Georgetown University Press / Washington, D.C.

Library of Congress Cataloging-in-Publication Data

♾ This book is printed on acid-free paper meeting the requirements of the

American National Standard for Permanence in Paper for Printed Library Materials.

19 18 17 16 15 14 13 12 9 8 7 6 5 4 3 2
First printing

CHAPTER 9

Persistent Enemies and Cyberwar

Rivalry Relations in an Age of Information Warfare

Brandon Valeriano and Ryan Maness

Introduction

In October 2010 the US Cyber Command was constituted as an active military four-star command. The 2010 National Intelligence Annual Threat Assessment states that the United States is "severely threatened" by cyber attacks.[1] With the increased importance of wars involving nonstate actors, the increase in the number of internal conflicts, and the scope of globalization, some scholars conclude that war and foreign policy has changed since 9/11.[2] The belief that war has changed is bolstered by the conjecture that cyberspace is now an important military battlefield. The field of security studies might be considered to be at a crossroads due to these perceptions.

Since the beginnings of armed conflict, enemies and combatants have always used the latest technology available to them to gain an advantage. Examples abound of states using technology, digital communication, and scientific espionage to challenge rivals. The difference now is that technology is the battlefield and the tactic at the same time. There is little to disconnect the means and objectives of cyberwar and cyber combat. This potential shift or revolution in foreign policymaking has to be evaluated on these terms. Has cyberspace become the battlefield, and what evidence do we have that this shift has changed relations between states? Yet very little has been done to study the actual impact of new tactics and weapons in the modern international battlefield. What is the true impact of cyberwar on the dynamics of conflict and interstate relations? This important question motivates our study in this volume.

This study will focus on persistent enemies or rivals. Interstate rivals are those states that perceive the other state as a threat and view interstate relations as a zero-sum game.[3] Vasquez defines rivalry as a "relationship characterized by extreme competition, and usually psychological hostility, in which the issue positions of contenders are governed primarily by their attitude toward each other."[4] To this point the data suggest that such pairs of states have experienced the most war in the interstate system since the end of the Napoleonic wars.[5] If one were to predict who will fight whom in the future and which states have realistic security threats, then scholars should rightly focus on rivals as the main unit of interest.[6] This study follows this advice and examines the impact of cyberwar or cyber tactics on the dynamics of rivalry.

This chapter will examine the theoretical and empirical impact of cyber strategies on rivalry relations. What sorts of behavioral expectations can we derive from a theory of information warfare during a rivalry? Our research path follows two lines of questioning. First, which rivals have cyber capabilities? To examine to the extent that informational battle tactics have changed diplomacy and military relations in the modern era, we must first examine the state of actual cyber capabilities. Do rivals have cyber-combat units, and if so, are these units tasked to target rivals or possibility, inflated threats?

Our second question is what impact cyber capabilities have on rivalry relations. If a state has a cyber unit tasked to target a rival, does this operation actually affect interstate relations? To accomplish both tasks we will present an examination of a few cases that explore the reach of cyber strategies in modern military structures among the rivalry population. How deeply have cyber capabilities and tactics penetrated rivalry dynamics? If there are cyber capabilities evident, do these tactics escalate tensions?

These research questions are important if one is to examine and theorize about the extent and impact of cyber tactics in modern international relations. Before policymakers can discuss the need for cybersecurity or the coming danger of cyberwar, we must first understand the true nature of cyber conflict against dangerous and long-standing enemies. The study of cyberwar must move away from the study of conjecture and fears of the possible and into the study of actual modern enemies' capabilities. This step is important, and this research effort is the first to examine both the theoretical and empirical impact of cyber technologies on conflict dynamics.

The chapter will proceed to define the domain of our analysis—cyber conflict—and then move toward an examination of the importance of rivalry studies. Based on other models of conflict, we will then theorize about the impact of the cyber tactics of rivals. Finally, our study will then answer the critical question of who has cyber capabilities and what impact these capabilities have on modern rivalry relations at this point.

Cyberwar and International Relations

For our purposes, cyberspace is physical; that is, it has defined boundaries of mainframes, wires, hard drives, and networks. Herb Lin explained the technical dimension

of cyber attack in chapter 3, but it is important to know that the cyber world is restricted to the domains of human thought. Computer science and math can only provide so many avenues of storage and information processes (despite the view of movies such as *Tron* and its sequel). Software tends to persist despite its faults; hence, we see the constant use of common programs (Windows) and platforms (Macs).

Perhaps the most important distinction of cyberspace is between the physical layer and syntactic layer.[7] These layers are not collapsed together. The danger coming from cyber invasions can only apply to the knowledge existing in the information world and not to all knowledge. In other words, a state is only as vulnerable as it allows itself to be.

The common usage of the term cyberwar seems to indicate direct battle between computational technologies and actors. The term's true intent is to suggest there is an ongoing technological battle in the context of a foreign policy interaction. This point is critical because we are talking about cyber technologies as used in war, battles, and foreign policy interactions rather than a futuristic war to take informational territory or further a cyber ideology. Cyberwar is generally the term used for a state's offensive capabilities and actions in cyberspace.[8] Hersh defines cyberwar as the "penetration of foreign networks for the purpose of disrupting or dismantling those networks, and making them inoperable."[9] Therefore, we define cyberwar as the use of computational technologies on the military or diplomatic battlefield of international affairs and interactions, whereas cybersecurity is the term used for a state's defensive (and sometimes offensive) capabilities in cyberspace.

As discussed in chapter 1, cyber attacks take the form of denial-of-service attacks, website defacement, and malicious code. All of the methods have the potential of doing real physical damage to states' infrastructure, secure government sites, or military operations. Malware is the most potent form of cyber warfare and should be the type most commonly used by rivals. But malware typically can only be used as a tactic if the target allows access. Malware generally works hand in hand with phishing attempts to gain passwords to access systems. Other forms of malware, such as the 2008 thumb-drive attack on the US Department of Defense network, require the physical insertion of the software into a disconnected network.

Most scholars suggest that cyber techniques change the character of war. Their line of logic is that the type of tactic or weapon used changes the nature of war because of its potential for devastating effect. What scholars must study is the impact of techniques on relations or outcomes rather than the possible impacts of said tactics. The focus must be made toward the observable and quantifiable rather than the suggested, inflated, or perceived fears that come from modern technologies.

To this point, studies about the impact of cyber technologies on foreign relations are purely speculative (as Patrick Jagoda reminds us in chapter 2). When one wants to advocate a position, the cyber challenge is put as a life-or-death struggle with immense implications for the modern nation-state. As Lynch puts it, "a dozen determined computer programmers can, if they find a vulnerability to exploit, threaten the United States' global logistics network, steal its operational plans, blind its intelligence capabilities, or hinder its ability to deliver weapons on target."[10] One can take such quotations and imagine the nuclear fallout created by self-aware artificial

intelligence made famous by *The Terminator* franchise. Our view is much different. Rather than suggest that the nature of combat has changed, we are interested in measuring if, how, and why it has changed.

Theoretically, our concern is with how cyber tactics are perceived in the enemy and the impact of the use of these tactics. Cyber tactics could destroy command-and-control structures in the military, wipe out the media apparatus of a state, destroy financial memory and wage economic combat, target the health industry and hospitals, or wither the ability of domestic units to protect the citizenry by eliminating technology used by police and the FBI. However, all these impacts are purely speculative. We do know, however, that there is a value to chaos in the enemy. By potentially destroying one's ability to respond, coordinate, and reciprocate attacks, intensive damage is done. Fear is the motivating mechanism for much of what occurs in the international arena, and cyberwar is no different. Cyber tactics could do damage, but the fear that these technologies engender is probably more important than any theoretical conjecture a pundit can make.

The real utility in cyberwar seems to be much more benign than is usually believed. The added value of cyber tactics is that these options tend to be low-penalty options. Information can be stolen, money can be moved around electronically, chaos can ensue through the activation of computer viruses, but these outcomes fail to compare to damage done by large-scale military options or even economic sanctions. Since most military networks are decentralized, the installation of malware is a difficult proposition. The question is really whether, in the future, military networks are going to strive for more integration or move prudently toward a path of isolation. The 2010 Stuxnet worm that seems to have hit the Iranian nuclear program had to be planted from the inside with traditional intelligence operatives, and most people overestimate hackers' ability to carry out large-scale attacks from a single computer.

In terms of conflict operations, the attractiveness of the target in relation to the capability used is a critical equation rarely examined. What good would a cyber attack be if it does little actual damage to a rival state? Much is made about the secret nature of cyber operations, but this can only be true in nonwarfare, nonrivalry situations. If Russia is invading Georgia and the entire information infrastructure of Georgia is destroyed, it is pretty clear who the aggressor is. Risk to the attacker in relation to the impact of the tactic does not make the use of cyber strategies a very rational option on the battlefield.

The Importance of Interstate Rivalry

The concept of rivalry brings history and historic interactions back into the study of political science. War is obviously not an isolated event that arises from a discrete set of events, yet this is how the field studies the event statistically. To understand why wars or crises develop, one must look at the entire past history of interactions

at the military, diplomatic, social, and cultural levels. Rivalry is simply defined as long-standing conflict with a persistent enemy.

Time is a key consideration for a rivalry. For a rivalry to exist, there must be a long history of events leading up to the situation. Rarely in international history do wars arise out of thin air or from quickly sparked events. When conflict does occur, there is likely a long-standing ancient and recent history of animosity that pushes both sides toward combat.

The next important consideration for rivalry is relative positions. As evidenced in the Vasquez definition of rivalry provided earlier, the issue positions of the contenders engaged in a rivalry are made in relation to the attitude of the other side.[11] Foreign policy perspectives during a rivalry are not made out of self-interest or rational planning but out of the simple consideration of denying a gain to the enemy. Rivals are in some ways addicted to perpetual conflict because of their singular outlook targeting the enemy. This perpetual competitive relationship is a dangerous situation in international affairs due to the buildup of hatred and tension over time.

The singular focus on the enemy also leads to another important consideration: the tendency of rivals to seek to "burn" the other side.[12] In a rivalry, the phrase "to cut off the nose to spite the face" comes to mind. A state engaged in a rivalry will likely harm its own security or people in order to support a wider collective struggle against an enemy.

Statistically, rivals tend to experience the most amount of conflict in the international system.[13] Whether this is an artifact of dataset construction is a debate that is ongoing, but William Thompson gives us greater confidence in the proposition that rivals are likely to fight again in the future.[14] But it is clear that a small amount of dyads in the interstate system experience an increased rate of warfare and conflict.

It then must be asked why rivals are so important in international relations? Rivals can tell us who will fight in the future but also—and more importantly—who to focus conflict reduction and resolution practices on in the present. These rival states are those that are most "at risk." Diehl and Goertz identify rivals as those states that have experienced a certain amount of militarized interstate disputes (either three or six disputes, depending on the level of rivalry under consideration).[15] William Thompson codes rivals based historical source and the mutual recognition of the other as an enemy. Much work has been done on why rivals fight or how rivarlries start, but little work has been done on the changing nature of warfare and rivalry.[16]

The Theoretical Impact of Cyberwar on Rivalry

During a rivalry, tensions are heightened and conflict is likely when there is a disagreement about the fundamental issues at stake in a foreign policy portfolio. The question for this chapter is what might be the impact of cyberwar on rivalry relations? Cyberwar is a tactic used to gain an advantage either diplomatically or militarily against a target. During a rivalry, all options should be on the table. Even war

becomes a viable foreign policy option, but here we are more interested in what the impact of cyber tactics will be on the escalation toward war.

Escalation to war in a rivalry typically occurs after a certain number of high-tension events occur in a rivalry relationship. The interesting thing about rivals is that they tend not to like launching offensive operations first, lest they be accused of starting a conflict in the first place. The normal relations range for a rivalry interactions tend to take the form of espionage, war games, brinksmanship, and economic warfare.

Due to the nature of rivalry, we should expect that cyber tactics are frequently used because these options are short of war and allow for plausible deniability as to the origin of attacks. While everyone might know where the attack is coming from, few have direct evidence of cyberwar as a foreign policy choice when compared to more overt military options. Cyber tactics will tend to be the "first shot fired" in a rivalry relationship. Due to the low cost of operations and advantage they might gain for the offensive side, the use of these tactics should be widespread in a rivalry relationship. Yet the challenge of attributing a cyber attack may facilitate covert actions against rivals.

Our theory is that cyberwar tactics are used during a rivalry. When these tactics are used, they should exacerbate the rivalry and result in the escalation of tensions between the states engaged in the operations. The value of chaos and fear is a key issue for cyber strategies in international relations. The ability to launch offensive cyber attacks alone might be enough to modify the behavior of a state. Attaining a minimal level of security to deter a large-scale cyber attack could motivate an enemy to launch a cyber technology arms race to gain the upper hand. The cyber race, like other arms races, reduces confidence and escalates tensions in a dyad.[17] Cyber rivalries should heighten tensions and lead to the breakdown of cooperation. Cyberwar is unlikely to trigger conventional war, but these operations could be leading sources of discontent between enemies and could lead to the escalation of conflict between the states engaged in such practices.

The counter hypothesis is that cyber tactics as used in a rivalry neither exacerbate tensions nor degrade confidence in the states engaged in the action. Cyberwar might be part of what Azar called the normal relations range for a rivalry.[18] Cyberwar is expected to occur and even tolerated as long as total offensive operations are not conducted. By total offensive operations, we mean direct attacks that might lead to the destruction of the energy infrastructure of a state or attacks meant to take control of army units. These options should be off the table for rivals because they will lead directly to war and therefore must never be tolerated; generally neither rival wants to be seen as the aggressor. The surprising finding in relation to conventional wisdom could be that rivals will tolerate cyberwar operations if they do not cross a line that leads directly into the loss of massive life.

"The Heavyweights"

There are only a few cyber "heavyweights" recognized by cyberwar experts of the international community.[19] Among these are the United States, China, Russia, Iran

and Israel.[20] The United States is the most "plugged-in" when it comes to reliance on the Internet for infrastructural and governmental services. Therefore, the United States is most frequently attacked by potentially malicious software. Furthermore, as the world's hegemonic power, the United States is also the main target state that dissident groups, terrorists, and rogue states wish to damage. Almost all Internet infrastructures are now connected to the Web in the United States, thus making the number of targets for cyberwar activity nearly unlimited. The United States is also one of the leading states in terms of the number of active rivals.[21] Thus, the expectation is that the United States, with its dependence on the Web, would have advanced cyber defenses, with the government playing a leading role in the protection of both private and public domains. However, this is not the case.

The United States is also known as the most offensively capable state in the realm of cyberwar.[22] American hackers are heavily recruited by government agencies such as the Department of Defense and Department of Homeland Security. There are also numerous private employment opportunities. This is not to say that the United States is free of cybercriminals; rather, the options for Americans with these skills to find legitimate work are more prevalent than in other nations with cyberwar capabilities. Russia and China, for example, do not have the number high-tech jobs available as in the United States, nor do they have the American Constitutional constraints that a free society may have. The expansive capabilities of American cyber agents are a frightening enemy for any state that chooses to pursue a cyberwar with the United States.

As Nigel Inkster highlights in chapter 12 of this volume, China has been gaining clout on the international stage in recent decades, and sees itself as a new force with which to be reckoned. Because China is aware that it is no match for the United States in conventional military terms, China has turned to a policy of managing this asymmetric gap by alternative means with the capabilities it has at hand. Some of these capabilities lie in cyberspace, and the Chinese have proven their worth in this domain. Chinese hackers are both homegrown and specially trained in universities.

Along with offensive cyber capabilities comparable to those of the United States, the Chinese government also has complete control of its Internet infrastructure.[23] If China were to come under a serious cyber attack, the government could shut off access to all international Web portals, thus containing and suppressing the attack. This capability is not something that the United States can claim because the multiple access points are privately owned by a number of diverse firms over which the government has no control. Therefore, in terms of cyberwar capabilities, it can be argued that China has a definite advantage over the United States.

Nevertheless, we have a problem with a potential cyber conflict between the United States and China; these two countries are not considered to be rivals under any rivalry dataset. There is no history of serious disputes on the level of historic examples such as the United States and the Soviet Union or India and Pakistan. Despite claims by pundits, China and the United States are not on a collision course. China's main foreign policy objective seems to be economic expansion, and there is little chance it will be able to compete militarily or economically with the United

States in the near future.[24] If the two main heavyweights often thought to be likely to fight in the near future are not rivals and are thus unlikely to fight, what danger is there from their immense cyber capabilities?

Russia is another state that has ambiguous cyberwar capabilities and policies. Russia boasts a highly educated and technically skilled workforce; however, the number of jobs that cater to these skills are few and far between. Furthermore, Russian culture demands a high degree of nationalistic pride, as the glory of the recent Soviet past still looms large in the hearts and minds of most Russians. Therefore, this combination of few jobs in the Russian private economy for high-tech skills along with Russian national pride has created a black market of hacking communities that have a potent ability to inflict damage on states. Nick Gvosdev offers a good explanation of this in chapter 11 of this volume. The potential of offensive Russian "hacktivism" is thus real, and its potential to do great damage is apparent.

The Islamic Republic of Iran is a semiclosed state that has great control over content of the Internet channels coming in and out of the country.[25] During the mass protests over the controversial 2009 elections, the Iranian government was successful in shutting out the opinions from the outside world on the Web, especially from the West. Iran is a state that can and will use the Web to control and censor its people. Iran is clearly a rival of the United States, at least in terms of foreign policy objectives.

Iran does have cyberwar capabilities but perhaps not as advanced as those from the United States, China, Russia, and Israel. Because Iran is a fundamentalist state that supports the expulsion of the Zionist state from the Holy Land, the country has been known to help Hamas and Hezbollah with their cyber campaigns against Israel. The Ashiyane Security Group is a covert Iranian hacking community that has hacked into more than four hundred Israeli websites, including those belonging to members of the Israeli Defense Ministry.[26] However, these attacks have only been DDoS and website defacement attacks, which cause mischief and disruption but are nowhere near as potent as the various types of malware.

Israel is becoming known as the most advanced cyber-capable state in the world.[27] The Israeli government has extensive networks of both offensive and defensive cyberwar technologies. It also actively supports Israeli "cyber patriots," private citizens with necessary technical skills who wish to help protect Israeli cyberspace from attacks by its many enemies in the Middle East, including Iran.[28] Israel's most recent and most infamous cyber attack is the September 2010 Stuxnet worm, which targeted the Iranian nuclear facilities as well as other important plugged-in infrastructure facilities. There is speculation on Israel's guilt in this attack; the United States has also been blamed, but neither country has claimed responsibility. However, behavior by diplomats from both Israel and the United States suggests that they are not denying responsibility either.[29]

Cyberwar between rivals may be more covert than vocal, and the data presented in the next section will help answer our primary question of how cyber capabilities are used in interstate rivalries. Table 9.1 is an outline of cyber capabilities as adapted from Clarke and Knake. This table ranks on a scale of 10 each country's offensive

TABLE 9.1
Overall Cyberwar Strength

Nation	*Cyber Offense*[a]	Cyber Dependence[b]	Cyber Defense[a]	Total Score[c]
Iran	4	5	3	12
United States	9	2	4	15
Israel	8	3	4	15
China	5	4	6	15
Russia	7	5	4	16

[a] On a scale of 10, with 10 being the strongest.
[b] On a scale of 10, with 10 being the least dependent.
[c] On a scale of 30 with 30 being the most vulnerable.
Source: Adapted and modified from Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), 148.

and defensive capabilities as well as its dependence upon cyberspace. Cyber dependence is ranked in reverse order; the higher the number, the less dependent the state is on computer technologies. The United States gets a low score because of how "plugged-in" it is to the Web for important infrastructural needs such as electricity and water. Therefore, the more dependent a state is on cyber technology, the more vulnerable it is.[30]

The football proverb "you can't have a good offense without a good defense" comes to mind here. The United States has the most powerful cyber arsenal in the world, but at the same time is heavily dependent upon the Internet and has relatively weak defenses from attack because it is not possible to "shut off" the Internet. Israel is similar to the United States in most respects but overall is not as dependent on cyber technologies as the United States is. Russia and China, on the other hand, are more balanced in terms of offensive and defensive capabilities. Although these nations are not as offensively capable as the United States is, they are able to defend themselves more readily against attack due to the fact that the government controls the important infrastructural lifelines of cyberspace. Iran falls somewhere on the lower end of the scale because it has very few offensive capabilities but is also less dependent overall and remains in control of access points. With capabilities defined, we will examine two case studies where capable rivals could wreak havoc on their adversaries.

Cyberwar in Rivalry: Case Examinations

The states mentioned earlier have robust, advanced cyber capabilities. Therefore, it is expected that these countries would use these capabilities against their rivals as

part of their foreign policy to weaken or destroy the capabilities of their adversaries. Rivals might wish to embarrass or demoralize their adversary publicly so that the adversary knows exactly where the attack comes from, and to claim credit, thus exerting power over the adversary. Animosities between rival states are largely vocal and exposed; thus, it would be expected that cyber attacks between rivalries would not be covert but rather open and public. Furthermore, it would also be expected that cyber attacks during a rivalry would increase tensions and push the states toward war.

Two ongoing and well-established contemporary rivalries that are chosen for this chapter are the dyads of Russia–Georgia and Israel–Iran. These rivals were extracted from the datasets on rivals by Klein, Goertz, and Diehl and by Thompson because they represent some of the heavyweights mentioned earlier, and because these dyads are the most often discussed by news pundits as being engaged in cyber combat.[31] It is important to study rivals who have cyber capabilities so that the possible effects of cyberwar are observed because we theorize that rivals will be more willing to use these capabilities on each other.[32]

Russia and Georgia

Russia and Georgia have been through many disputes since the fall of the Soviet Union. Tensions came to a head when Russia invaded Georgia on August 8, 2008.[33] The war lasted five days and ended with an overwhelming Russian victory.[34] There were many events leading to Russia's invasion, which centered on South Ossetia and Abkhazia. First, the nature of South Ossetia and Abkhazia were disputed. Second, there were minor skirmishes between Russian and rebels troops; eighteen events have been counted during the five days.[35] Third, Russia has used its energy policy to throw its weight around with the countries of Europe, including Georgia.[36] Finally, it has been argued that because of the uncertainty of the Black Sea Fleet's fate in Crimea, Russia was looking for a new Black Sea port through Abkhazia.[37] Given that the 2008 war occurred in the information age, it is important to examine the role cyber capabilities played in this rivalry.

As the data show, although these adversaries have advanced and potentially catastrophic cyber capabilities, use of these weapons has been minimal and the credit claimed for the attacks has not been from the governments of these states. Rather, for the most part the "buck has been passed" to nonstate actors and the cyber underground. Table 9.2 shows data of cyber attacks between the two dyadic rivalries from the past ten years. The attacks were minimal by cyber standards, as only DDoS and website defacements were employed. The Russian government denied any involvement in these attacks, instead passing the blame to Russian patriots sympathetic to the cause. Russia has the ability to inflict more damage on Georgian cyberspace; however, it chose not to. Georgia retaliated by flooding certain government sites with DDoS attacks, but the damage was minimal and temporary at best. Therefore, the full use of cyber warfare tactics is yet to be part of the Russian or Georgian

TABLE 9.2
Cyber Attacks between Russia and Georgia

Date	*Direction*	*Title*	*Type*	*Damage*
8/2/2004	Russia>Georgia	Massive Keystroke Logging Attack	Malware (keystroke logging)	Massive information theft
8/12/2008	Russia>Georgia	Russian Invasion Cyber Attacks	DDoS, website defacements, malware (logic bombs)	Disruption and defacement of government websites, erasure of data in military sites
8/12/2008	Georgia>Russia	Retaliation for Russian Cyber Attacks	DDoS	Disruption of various public and private Russian sites

Source: Google News: Keywords "Russia Georgia Cyber," accessed December 9, 2010.

arsenal, even in times of physical conflict. Most damage was done by Russian and Georgian guns, not cyber attacks.

The cyber attacks that accompanied this five-day war were merely disruptions in Georgian and Russian Internet service as well as defacements of various government websites. What came out of the war was the recognition by Russia and its Commonwealth of Independent States allies of Abkhazia and South Ossetia as independent states, denouncement of Russian actions by the West, and increased tensions between the rivals. The effects of the cyber attacks on the rivalry escalation were minimal at best.[38]

Israel and Iran

The rivalry between Israel and the Islamic Republic of Iran began in the aftermath of the Iranian Revolution of 1979, when religious fundamentalists took control of Tehran and have been in control ever since. Israel became the sworn enemy of Iran, and the rivalry has been escalating because of the Iranian regime change.[39] Iran has been the most vocal supporter of the Palestinian state and has vowed to see the Zionist state wiped off the face of the Earth. Iran remained rather benign in the 1980s when it came to front-line attacks (physical or rhetorical) on the Israeli–Palestinian peace process. However, beginning in the 1990s the state began to more directly undermine the Israeli–Palestinian peace process and to fund anti-Israeli terrorist groups such as Hamas and Hezbollah.[40] Terrorist attacks on Israel funded by Iranian money are too numerous to discuss in this chapter. Espionage and assassinations have been the catalyst for Iranian animosity against Israel. In this new era of supposed cyberwarfare, espionage, and terror, it has been found that this may be the new realm where the Israeli–Iranian rivalry escalates. The animosities of these two dyads could see unconstrained and unrelenting cyberwar.

Only in the past two years have the cyber tactics between the rivals of Iran and Israel escalated. Earlier, these attacks had been limited to DDoS attacks and website defacements in reaction to certain foreign policy choices. The first three events in table 9.3 represent only minor incursions in each others' cyberspace. "Electronic Jihad" and "Cyber Jihad" were joint efforts by the Iranian government and various anti-Zionist terrorist groups such as Hezbollah. These were reactions to Israeli policies toward the disputed Palestinian territories of Gaza and the West Bank. Tensions increased on both sides because of these events; however, the role of cyber attacks in the heightened tensions remains to be seen. Many issues exist between the rivals; therefore, any action taken by either side could possibly escalate to conflict.

Retaliation against the Iranian government's 2006 sponsorship of an online contest that poked fun at the existence of the Holocaust was one of the first cyber attacks in which Israel directly targeted Iran. Israeli hackers flooded the website until it was for all intents and purposes shut down. The contest never declared a winner, but Israel was relentless in its attack on Iran. The Iranian government denied sponsoring the online event, but sources point to Iranian president Mahmoud Ahmadinejad as the mastermind behind the idea.

TABLE 9.3
Cyber Attacks between Israel and Iran

Date	*Direction*	*Title*	*Type*	*Damage*
9/1/2000	Iran>Israel	Electronic Jihad	DDoS	Disruption of service, lost time and money
8/1/2001	Iran>Israel	Cyber Jihad	DDoS	Disruption of service, lost time and money
2/7/2006	Israel>Iran	Iran Holocaust Cartoon Contest	DDoS, website defacements	Disruption of web-based cartoon contest in Iran
10/27/2006	Iran>Israel	Israeli-Lebanon Conflict	DDoS	Disruption of service, lost time and money
12/272008	Iran>Israel	Operation Cast Lead Retaliation	DDoS, website defacements	Disruption of Israeli government sites
7/7/2009	Israel>Iran	Nuclear Facilities Virus	Malware (virus)	Disruption of communications, theft of secret information
9/30/2010	Israel>Iran	Stuxnet	Malware (worm)	Disruption of Iranian nuclear facilities, destruction of centrifuges

Source: Google News: Keywords "Iran Israel Cyber," accessed December 9, 2010.

Cyber attacks began to heat up between the rivals in 2008 with the Israeli invasion of Lebanon in response to short-range missile attacks by the terrorist group in northern Israel. Again, as with the Russia–Georgia dyad, cyberwarfare was a supplement to physical attack, not the primary weapon that caused the most damage. The DDoS attack was a joint effort by Iran and other pro-Palestinian governments as well as nonstate actors such as Hezbollah and Hamas. Defacing of government websites and flooding of important Israeli commercial websites until they shut down was the damage done. The tables would be turned on Iran in 2009 and 2010, when some of the most sophisticated malware released on a state's infrastructure manifested itself.

Because of Iran's nuclear ambitions, Israel has stepped up its cyberwar against its rival. Only in 2009 did Israel begin using malware against Iran. The Nuclear Facilities Virus was malware intended to steal information from top-secret government sites as well as disrupt communication between parties working in Iran's nuclear program. Iran has pointed the finger at Israel and the United States and has denounced the attack in typical Iranian anti-Zionist fashion. Both governments have denied that the attack originated in their cyberspace. Nevertheless, tensions have increased within the rivalry.

The most recent worm released on Iran's network in 2010, Stuxnet, is becoming known as the most ambitious and most damaging piece of malware released into a state's infrastructure. Recent evidence has shown that the worm was developed in Israel, but where it was released has still not been pinpointed.[41] This worm has destroyed Iranian centrifuges and has severely disrupted the progress made by Iranian nuclear scientists. The genius behind the worm is that it only became malicious when specific targets, the Iranian centrifuges, were activated. It told the centrifuges to spin out of control, effectively destroying them. Furthermore, the worm sent code to the Iranian facilities' control panels to indicate that everything was operating smoothly while the centrifuges were destroying themselves. Reports estimate that the Stuxnet attack has set back Iran's nuclear program by at least three years.[42]

Iran has yet to retaliate, but maybe Stuxnet is the beginning of a new age of more malicious and more destructive cyberwar. Iran has vowed to beef up its cybersecurity as well as its cyber-offensive capabilities as a result of the Stuxnet attack. However, Iran does not have the domestic manpower to mount such sophisticated attacks as Stuxnet, and how this new "beefing up" of Iranian cyber capabilities provokes Israel or the United States remains to be seen.[43] Furthermore, the assassinations of Iranian scientists and the threat of airstrikes seem to more effective at getting Iran's attention than this most recent malicious Stuxnet worm.

Assessment of Case Examinations

Why have these very vocal and much-hated rivals failed to take credit for these minimal attacks that one would assume they would be proud to take credit for? Several

reasons come to mind, which have implications for the future of cyberwarfare between rivals and the international community in general.

Cyber Constraints

Perhaps a reason for the relevant lack of serious malware attacks between rivals is fear of retaliation from the other side. If a state within a rivalry openly and blatantly attacks its adversary's infrastructure or secret government databases, that state may perceive the attack as it would a physical attack such as an airstrike or infantry invasion. Attacks like these are considered acts of war, and it is likely that these states are not quite ready or willing to escalate the rivalry to this point. Israel may have the malware available to completely destroy Iran's nuclear program, but the repercussions of this action may escalate to all-out war between the countries, which could very well escalate to include major powers such as the United States and China. Therefore, cyberwarfare may not have escalated to more harmful attacks in the same way nuclear deterrence allowed for peace between major powers during the Cold War. Neither adversary wanted to act first and be blamed for causing World War III.

Cyber Norms and a Normal Relations Range

The rules and norms in the realm of cyberspace have yet to be determined, but it does seem clear that rivals operate as rivals should. They are able to manage their tensions in such a way as to forestall violence for long periods. The rules of the game in cyberspace have yet to be determined, and states have yet to employ blatant widespread damage via the Web out of fear of the unknown or disturbing the balance of harmony during a rivalry. Surprisingly, Russia has pushed for treaties among the international community that would set up norms of cyberwar among states. The European Union has also promoted this idea. However, the United States and China are major powers that are skeptical about signing on to such agreements.[44] These skeptics are the roadblocks to more talks about an agreed-upon mode of behavior by adversaries in cyberspace.

Plausible Deniability

States with cyber capabilities also have the advantage of being able to deny any involvement by cyber attacks originating within their borders. Because cyber attacks are difficult to trace, and even more difficult to trace to a government, states that may have sponsored or coordinated a cyber attack against its rival will have the advantage of plausibly denying any involvement in a malicious breach of security. For example, the website defacements and DDoS attacks perpetrated by Russia and Georgia during the 2008 wars were blamed on the patriotic nonstate actors sympathetic to each side's cause. Cyber-attack denial by states actively involved in a physical war is puzzling, especially since the purpose of war is to get the other side's

government to capitulate to demands. Either the Russians and Georgians were telling the truth, or the cyber constraints and lack of cyber norms discussed earlier played a part. Russia perhaps feared retaliation by the United States, and Georgia perhaps feared escalated Russian attacks.

As of this writing, the Stuxnet worm, it appears, is the work of a joint Israeli–American effort. Although diplomats and representatives from both governments are officially denying involvement in the development and deployment of the worm, they do so with what can be interpreted as a metaphorical "wink" in that they were unofficially involved.[45] They state their pleasure with the fact that Iran's nuclear program has been set back because of the worm but will not cross the line in blatantly admitting their involvement. Thus far, it has been rare that a government has openly admitted to committing acts of cyberwar.

Lack of "Shock Value"

The September 11, 2001, attacks were a spectacle that changed the course of American foreign policy and put the world on high-alert ever since. Visuals of the burning Twin Towers and Pentagon are ingrained in the mind of every American old enough to remember. These physical attacks propagated by terrorists have had lasting "shock value" that has changed the behaviors of major states. Cyber attacks, on the other hand, may not have the shock value that a conventional physical attack may demonstrate. Therefore, in order to get rivals to capitulate to a state's demands, an airstrike, artillery strike, or all-out invasion may get the desired outcomes that rivals are looking for. Cyber attacks, although potentially lethal, do not have the same "punch" as a physical attack. Russia's cyber attack in 2008 was accompanied by a major military campaign, and Georgia quickly surrendered because of the bullets, not the botnets. Furthermore, Israel still has not ruled out extensive airstrikes on Iran's nuclear facilities, even though the Stuxnet worm that Israel has been accused of releasing has set back the Islamic Republic's nuclear ambitions.

The attacks in cyberspace between the rivalries of Russia and Georgia and Iran and Israel have been limited, constrained, and denied. These covert methods of attack are equivalent to a twenty-first-century version of a very ancient form of foreign policy—spying. Gathering information from and sabotaging valuable infrastructure of enemies has been part of human history since the advent of warfare. Thus far, this form of spying has yet to be normalized, and because of this, the true nature of states' cyber capabilities has yet to be realized. Rivals tend to not use cyber operations very often, and when they do, these operations do not exasperate tensions beyond a normal relations range. Escalation of malicious attacks are very possible and may be apparent in the very near future; however, constraints, lack of norms, deniability, and lack of shock value have allowed for damaging yet limited cyberwarfare among rivals.

Assessment

This chapter is a preliminary evaluation meant to theoretically and empirically trace out the impact of cyber strategies on modern interstate relationships. Future work will go forward with quantifying the specific cyber capabilities of each state engaged in current rivalries. We can only know the true impact of a policy by studying its actual use in current foreign policy. It does little good to trump up a factor as a "game changer" before its true impact is even measured.

Seymour Hersh makes an interesting point in his contention that the danger expounded by cyberwar theorists results from a confusion between cyber espionage and cyberwar.[46] We have a similar finding in this chapter; rivals tend to use cyber tactics. However, these tactics are not widespread, nor do these tactics escalate tensions within a rivalry dyad.

This finding is surprising based on the increased attention cyber combat gathers in the realm of national security. Perhaps the dangers stated by various authors is overstated, extreme, or—even worse—arises out of self-interest in the need to perpetuate a national security state. The fear caused by cyber tactics is much greater than the actual danger such actions have posed in real life. Fear is the basis for rivalry, and as long as enemies fear the other side, any tactic that could inflict damage is frightening.

The Future of Cyberwar and Rivalry

The shadow of the future plays heavily on the issue of cyberwar. At this point, no one knows the limits in terms of targets during an all-out cyberwar, but our initial hypothesis that states with cyber capabilities and engaged in a rivalry will use all means necessary to counter said rival has been falsified at this point. The remaining question concerns the future. Will we continue to see low-level use of cyber technologies to target rival states?

The danger lies in Stuxnet becoming a harbinger of the future. If the goal of Stuxnet was to hamper the industrial capabilities of a target state, the United States is the most vulnerable to retaliation on this point. By opening up Pandora's Box in the context of Iran, Israel and the United States are now opening themselves to all sorts of attacks because they went beyond the normal taboos of cyber operations in rivalry to this point. A *New York Times* article on Stuxnet makes the point that the worm likely harmed Iran's nuclear production capabilities as much as a direct strike by Israel would have.[47] Does this mean that Iran will seek to retaliate and escalate the conflict?

All too often rivalries are seen as innocuous, just part of the foreign policy project for all states. The fear for us is that some of these managed types of rivalries might increase in hostility due to the actions on the cyber battlefield. To this point we have

seen little evidence of unrestricted cyber warfare against a rival, and we hope this trend continues. The future is very much dependent on how rival states react to actual conflict events launched by their enemies. On that point, the entire history of rivalry studies suggests that we have much to worry about because rivals tend to overreact to threats posed by enemies.

Notes

1. Dennis C. Blair, "Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence," February 2, 2010, www.dni.gov/testimonies/2010 0202_testimony.pdf.

2. Mary Kaldor, *New and Old Wars: Organized Violence in a Global Era* (Stanford, CA: Stanford University Press, 1999). Dissent to this perspective is offered by many who use data to analyze war and foreign policy. See Errol Henderson and J. Singer, " 'New Wars' and Rumors of 'New Wars,' " *International Interactions* 28, no. 2 (2002): 165–90.

3. Paul Diehl and Gary Goertz, *War and Peace in International Rivalry* (Ann Arbor: University of Michigan Press, 2000); and William R. Thompson, "Identifying Rivals and Rivalries in World Politics," *International Studies Quarterly* 45 no. 4 (2001): 557–86.

4. John Vasquez, *The War Puzzle* (Cambridge: Cambridge University Press, 1993).

5. Diehl and Goertz, *War and Peace in International Rivalry*; and Brandon Valeriano, "Becoming Rivals: The Process of Rivalry Development," in *What Do We Know about War*, 2nd ed., ed. J. A. Vasquez (Lanham, MD: Rowman & Littlefield, 2012).

6. Stuart Bremer, "Who Fights Whom, When, Where, and Why?" in *What Do We Know about War?* ed. J. A. Vasquez, 23–36 (Lanham, MD: Rowman & Littlefield, 2000).

7. Martin C. Libicki, *Conquest in Cyberspace* (Cambridge: Cambridge University Press, 2007).

8. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010).

9. Seymour Hersh, "The Online Threat: Should We Be Worried about Cyber War?" *New Yorker,* November 2010.

10. William J. Lynch III, "Defending a New Domain," *Foreign Affairs* 89 no. 5 (2010): 97–108.

11. Vasquez, *War Puzzle.*

12. Valeriano, "Becoming Rivals."

13. Diehl and Goertz, *War and Peace in International Rivalry.*

14. Thompson, "Identifying Rivals."

15. Diehl and Goertz, *War and Peace in International Rivalry.*

16. On whey rivals fight, see ?Michael P. Colaresi, ?Karen A. Rasler, ?and William R. Thompson, *Strategic Rivalries in World Politics: Position, Space and Conflict Escalation*, (?Cambridge: Cambridge University Press?, ?2007). On how rivalries start, see Valeriano, "Becoming Rivals."

17. Susan Sample, "Arms Races and Dispute Escalation: Resolving the Debate," *Journal of Peace Research* 34, no. 1 (1997): 7–22; Susan G. Sample, "Military Buildups: Arming and War," in *What Do We Know About War?* ed. J. A. Vasquez, 167–96 (Lanham, MD: Rowman & Littlefield, 2000).

18. Edward Azar, "Conflict Escalation and Conflict Reduction in an International Crisis: Suez, 1956," *Journal of Conflict Resolution* 16 (1972): 183–201.

19. Clarke and Knake, *Cyber War.*

20. Other countries include France, Ukraine, India, Pakistan, Belarus, Great Britain, and Germany.

21. Thompson, "Identifying Rivals."

22. Clarke and Knake, *Cyber War*.

23. Ibid.

24. Fareed Zakaria, *The Post-American World* (New York: W. W. Norton), 2008; and Daniel Drezner, "Bad Debts: Assessing China's Financial Influence in Great Power Politics," *International Security* 34 (Fall 2009): 7–45.

25. Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, 2010).

26. Ibid.

27. Ibid.

28. Ibid.

29. Ibid.

30. Clarke and Knake, *Cyber War*.

31. James P. Klein, Gary Goertz, and Paul F. Diehl. "The New Rivalry Dataset: Procedures and Patterns," *Journal of Peace Research* 43 no. 3 (2006): 331–48. Rivalry between the United States and China are not found in either dataset, so this dyad cannot be used for this study.

32. To locate and disseminate cyber attacks used with the Russian–Georgian and Israeli–Iranian rivalries, qualitative content analysis is used. Using the search engine Google News, we sifted through news stories reporting the instances of cyber attacks between the states. The keywords of "Iran Israel Cyber" and "Russia Georgia Cyber" were inputted, and the results are reported in the following.

33. Jim Nichol, "Russia-Georgia Conflict in South Ossetia: Context and Implications for US Interests" *Congressional Research Service Report for Congress*, October 24, 2008.

34. Ibid.

35. Gary King, "Ten Million International Dyadic Events" (2006). Accessed 1/20/2010, available at http://dvn.iq.harvard.edu/dvn/dv/king/faces/study/StudyPage.xhtml?studyId=505&studyListingIndex=0_ee2717d5514905203fbf4ce96055.

36. Shamil Midkhatovich Yenikeyoff, "The Georgia-Russia Standoff and the Future of Caspian and Central Asian Energy Supplies," *Middle East Economic Survey* 51, no. 36 (2008): 1–4.

37. Nichol, "Russia-Georgia Conflict."

38. Ibid, 17–19.

39. Trita Parsi, *Treacherous Alliance: The Secret Dealings of Israel, Iran, and the United States* (New Haven, CT: Yale University Press, 2007).

40. John P. Miglietta, *American Alliance Policy in the Middle East, 1945–1992: Iran, Israel, and Saudi Arabia* (Lanham, MD: Lexington Books, 2002).

41. William J. Broad, John Markoff, and David E. Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011.

42. Ibid.

43. Josh Lederman, "Iran Seeks to Boost Corps of Web Watchers," *Associated Press*, January 19, 2011, www.foxnews.com/world/2011/01/19/iran-seeks-boost-corps-web-watchers/.

44. Clarke and Knake, *Cyber War*.

45. Broad, Markoff, and Sanger, "Israeli Test on Worm."

46. Seymour Hersh, "Should We Be Worried About Cyber War? *New Yorker*, November 2010.

47. Broad, Markoff, and Sanger, "Israeli Test on Worm."