REPORT

FireEye

WORLD WAR C :

Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks

Authors: Kenneth Geers, Darien Kindlund, Ned Moran, Rob Rachwald

SECURITY REIMAGINED

CONTENTS

Executive Summary 3

Introduction 4

A Word of Warning 5

The FireEye Perspective 5

Asia-Pacific 6

Russia/Eastern Europe 12

Middle East 14

The West 18

Conclusion 21

About FireEye 22

Executive Summary

Cyberspace has become a full-blown war zone as governments across the globe clash for digital supremacy in a new, mostly invisible theater of operations. Once limited to opportunistic criminals, cyber attacks are becoming a key weapon for governments seeking to defend national sovereignty and project national power.

From strategic cyber espionage campaigns, such as Moonlight Maze and Titan Rain, to the destructive, such as military cyber strikes on Georgia and Iran, human and international conflicts are entering a new phase in their long histories. In this shadowy battlefield, victories are fought with bits instead of bullets, malware instead of militias, and botnets instead of bombs.

These covert assaults are largely unseen by the public. Unlike the wars of yesteryear, this cyber war produces no dramatic images of exploding warheads, crumbled buildings, or fleeing civilians. But the list of casualties—which already includes some of the biggest names in technology, financial services, defense, and government —is growing larger by the day.

A cyber attack is best understood not as an end in itself, but as a potentially powerful means to a wide variety of political, military, and economic goals.

"Serious cyber attacks are unlikely to be motiveless," said Martin Libicki, Senior Scientist at RAND Corp. "Countries carry them out to achieve certain ends, which tend to reflect their broader strategic goals. The relationship between the means chosen and their goals will look rational and reasonable to them if not necessarily to us."

Just as each country has a unique political system, history, and culture, state-sponsored attacks also have distinctive characteristics, which include everything from motivation to target to type of attack.

This report describes the unique characteristics of cyber attack campaigns waged by governments worldwide. We hope that, armed with this knowledge, security professionals can better identify their attackers and tailor their defenses accordingly.

Here is a quick overview:

- **Asia-Pacific.** Home to large, bureaucratic hacker groups such as the "Comment Crew" who pursue many goals and targets in high-frequency, brute-force attacks.
- **Russia/Eastern Europe.** These cyber attacks are more technically advanced and highly effective at evading detection.
- **Middle East.** These hackers are dynamic, often using creativity, deception, and social engineering to trick users into compromising their own computers.
- **United States.** The most complex, targeted, and rigorously engineered cyber attack campaigns to date.

Introduction

World War Z—a bestselling book and Hollywood movie—detailed a global pandemic in which politics and culture deeply influenced how the public—and by extension, governments—reacted to a zombie plague. In one passage, for example, an Arab boy refused to believe that the disease was real, suspecting that Israel had fabricated the story. The nations described in World War Z—the United States, China, Russia, South Korea, Israel, and many others—are involved in a very different type of conflict, but one with real and growing national security impact: World War C, where "C" stands for "Cyber". However, the same rule applies: each country has a unique political system, history, language, culture, and understanding of human and international conflict.

Cyber conflict often mirrors traditional conflict. For example, China uses high-volume cyber attacks similar to how it used infantry during the Korean War. Many Chinese soldiers were sent into battle with only a handful of bullets. Given their strength in numbers, they were still able to achieve battlefield victories. On the other end of the spectrum lie Russia, the U.S., and Israel, whose cyber tactics are more surgical, reliant on advanced technologies and the cutting-edge work of contractors who are driven by competition and financial incentives.

We are still at the dawn of the Internet Age. But cyber attacks have already proven themselves as a low-cost, high-payoff way to defend national sovereignty and to project national power. Many of today's headlines seem to be pulled from the pages of a science fiction novel. Code so sophisticated it destroys a nuclear centrifuge thousands of miles away. Malware that secretly records everything a user does on a computer. A software program that steals data from any nearby device that has Bluetooth connectivity. Encrypted code that decrypts only on one specific, target device. Such sophistication speaks volumes about the maturity, size, and resources of the organizations behind these attacks. With a few rare exceptions, these attacks are now in the exclusive realm of nation-states.

"The international community has developed a solid understanding of cyber technology," said Prof. Michael N. Schmitt of the U.S. Naval War College, in an email interview. "What is missing is a grasp of the geopolitical context in which such technology operates. Attribution determinations made without sensitivity to the geopolitical surroundings are seldom reasonable."

World War C, like any analogy, has its limits. Cyber war has been compared to special operations forces, submarine warfare, missiles, assassins, nuclear weapons, Pearl Harbor, 9/11, Katrina, and more. Even our zombie analogy is not new. Often, any compromised computer, if it is actively under the surreptitious control of a cybercriminal, is called a zombie, and botnets are sometimes called zombie armies. Also, compared to stockpiling tanks and artillery, writing cyber attack code, and compromising thousands if not millions of computers, is easy. Moreover, malware often spreads with the exponential growth of an infectious disease.

This report examines many publicly known cyber attacks. By exploring some of the distinctive national or regional characteristics of these attacks, organizations can better identify their attackers, anticipate future attacks, and defend themselves.

A Word of Warning

The analytical waters surrounding cyber warfare are inherently murky. At the strategic level, governments desire to have a degree of plausible deniability. At the tactical level, military and intelligence organizations envelop such operations in layers of classification and secrecy. To be effective, information operations rely on deception—and the Internet offers an ideal venue for a spy's smoke and mirrors. In practical terms, hackers often run their attacks through cyber terrain (such as compromised, third-party networks) that present investigators with technical and jurisdictional complications. And finally, cybercriminal tools, tactics, and procedures (TTPs) evolve so quickly that cyber defense, legislation, and law enforcement remain behind the attacker's curve.

"The biggest challenge to deterring, defending against, or retaliating for cyber attacks is the problem of correctly identifying the perpetrator," said Prof. John Arquilla, Naval Postgraduate School in an email interview with FireEye.® "Ballistic missiles come with return addresses. But computer viruses, worms, and denial of service attacks often emanate from behind a veil of anonymity. The best chance to pierce this veil comes with the skillful blending of forensic back-hacking techniques with deep knowledge of others' strategic cultures and their geopolitical aims."

Cyber "attribution"—identifying a likely culprit, whether an individual, organization, or nation-state—is notoriously difficult, especially for any single attack. States are often mistakenly identified as non-state actors, and vice versa. To make matters worse, ties between the two are increasing. First, a growing number of "patriotic cybercriminals" ostensibly wage cyber war on behalf of governments (examples include Chechnya and Kosovo in the 1990s, China in 2001, Estonia in 2007, Georgia in 2008, and every year in the Middle East).[1] Second, cybercrime organizations offer anyone, including governments, cyber attack services to include denial-of-service attacks and access to previously compromised networks.

FireEye researchers have even seen one nation-state develop and use a sophisticated Trojan, and later (after its own counter-Trojan defenses were in place) sell it to cybercriminals on the black market. Thus, some cyber attack campaigns may bear the hallmarks of both state and non-state actors, making positive attribution almost impossible. And finally, "false flag" cyber operations involve a hacker group behaving like another to mislead cyber defense researchers.

The FireEye Perspective

Within the shadowy world of cyber warfare, FireEye occupies a unique position. First, our threat protection platform has been installed on thousands of sensitive networks around the world. This gives our researchers a global and embedded presence in the cyber domain. Second, FireEye devices are placed behind traditional security defenses such as firewalls, anti-virus, and intrusion prevention systems. This means that our "false positive" rate is extremely low, and that the attacks we detect have already succeeded in penetrating external network defenses.

[1] Geers K. (2008) "Cyberspace and the Changing Nature of Warfare," Hakin9 E-Book, 19(3) No. 6; SC Magazine (27 AUG 08) 1-12.

Asia-Pacific

China—the elephant in the room

The People's Republic of China is the noisiest threat actor in cyberspace. The reasons for this include its huge population, a rapidly expanding economy, and a lack of good mitigation strategies on the part of its targets.

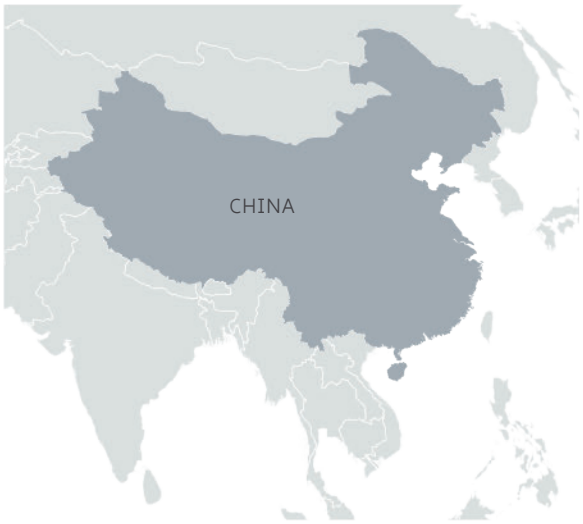
Chinese attacks on the U.S.

The list of successful Chinese compromises is long, and spans the entire globe. Here are some of the most significant incidents in the U.S.:

- **Government:** By 1999, the U.S. Department of Energy believed that China posed an "acute" threat to U.S. nuclear security via cyber espionage.2 By 2009, China apparently stole the plans for the most advanced U.S. fighter jet, the F-35.[3].
- **Technology:** China hacked Google, Intel, Adobe, and RSA's SecureID authentication technology—with which it then targeted Lockheed Martin, Northrop Grumman, and L-3 Communications.[4]
- **Business and Financial Services:** Morgan Stanley, the U.S. Chamber of Commerce, and numerous banks have been hacked.[5]
- **Media:** The New York Times, Wall Street Journal, Washington Post, and more have been targeted by advanced, persistent cyber attacks emanating from China.[6]
- **Critical Infrastructure:** Department of Homeland Security (DHS) reported in 2013 that 23 gas pipeline companies were hacked (possibly for sabotage)[7] and that Chinese hackers were seen at the U.S. Army Corps of Engineers' National Inventory of Dams.[8]

Some of these cyber attacks have given China access to proprietary information such as research and development data. Others offer Chinese intelligence access to sensitive communications, from senior government officials to Chinese political dissidents.

[2] Gerth, J. & Risen, J. (2 May 1999) "1998 Report Told of Lab Breaches and China Threat," The New York Times.
[3] Gorman, S., Cole, A. & Dreazen, Y. (21 Apr 2009) "Computer Spies Breach Fighter-Jet Project," The Wall Street Journal.
[4] Gross, M.J. (1 Sep 2011) "Enter the Cyber-dragon," Vanity Fair.
[5] Gorman, S. (21 Dec 2011) "China Hackers Hit U.S. Chamber," Wall Street Journal; and Ibid.
[6] Perlroth, N. (1 Feb 2013) "Washington Post Joins List of News Media Hacked by the Chinese," and "Wall Street Journal Announces That It, Too, Was Hacked by the Chinese," The New York Times.
[7] Clayton, M. (27 Feb 2013) "Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage," The Christian Science Monitor.
[8] Gertz, B. (1 May 2013) "Dam! Sensitive Army database of U.S. dams compromised; Chinese hackers suspected," The Washington Times.



Chinese attacks outside the U.S.

Of course, the U.S. is not China's only cyber target. All traditional, geopolitical conflicts have moved into cyberspace, and Chinese compromises encompass the entire globe. But many contests have been one-sided affairs, with all publicly known attacks emanating from China.

- **Europe:** In 2006, Chinese cybercriminals targeted the UK House of Commons;[9] in 2007, German Chancellor Angela Merkel raised the problem of nation-state hacking with China's President;[10] in 2010, British MI5 warned that undercover Chinese intelligence officers had given UK business executives malware-laden digital cameras and memory sticks.[11]

- **India:** Indian officials worry that China could disrupt their computer networks during a conflict. One expert confided that an exclusive reliance on Chinese hardware might give China a "permanent" denial-of-service capability.[12] One sophisticated attack on an Indian Navy headquarters allegedly used a USB vector to bridge the "air-gap" between a compartmentalized, standalone network and the Internet.[13]

- **South Korea:** The South Korean government has complained for years of Chinese activity on its official computers, including a 2010 compromise of the personal computers and PDAs belonging to much of South Korea's government power structure[14] and a 2011 assault on an Internet portal that held personal information for 35 million Koreans.[15].

- **Japan:** Here, the target list includes government, military, and high-tech networks. Chinese cybercriminals have even stolen classified documents.[16].

[9] Warren, P. (18 Jan 2006) "Smash and grab, the hi-tech way," The Guardian.
[10] "Espionage Report: Merkel's China Visit Marred by Hacking Allegations," (27 Aug 2007) Spiegel.
[11] Leppard, D. (31 Jan 2010) "China bugs and burgles Britain," The Sunday Times.
[12] Exclusive cyber threat-related discussions with FireEye researchers.
[13] Pubby, M. (01 Jul 2012) "China hackers enter Navy computers, plant bug to extract sensitive data," The Indian Express.
[14] Ungerleider, N. (19 Oct 2010) "South Korea's Power Structure Hacked, Digital Trail Leads to China." Fast Company.
[15] Mick, J. (28 Jul 2011) "Chinese Hackers Score Heist of 35 Million South Koreans' Personal Info," Daily Tech.
[16] McCurry, J. (20 Sep 2011) "Japan anxious over defence data as China denies hacking weapons maker," The Guardian;

Reconnaissance	Mailing Lists, Previous Watering Hole Intel, Crawling, Mining Social Networks
Weaponization	Masked EXEs to Appear Non-Executable File Formats, Malicious Non-EXE File Formats, Watering Hole Attacks
Delivery	Strategic Web Compromises, Spear phish URLs in Email, Weaponized Email Attachments, Webserver compromise via scanning
Exploitation	0-Day Browser / Application Vulnerabilities, Social Engineering
Installation	Feature Rich, Compact RATs with Minimal Evasion Capabilities (Requires Operator For Lateral Movement)
Command and Control (C2)	HTTP with Embedded, Standard Encodings (e.g., XOR), along with Custom Encodings
Actions on Objectives	Intelligence Gathering / Economic Espionage, Persistent Access
TTP Exemplars	Comment Group

Table 1: Characteristics of Chinese cyber attacks

- **Australia:** China allegedly stole the blueprints for the Australian Security Intelligence Organization's new $631 million building.[17]

- **Worldwide:** In 2009, Canadian researchers discovered that China controlled a worldwide cyber espionage network in over 100 countries.[18] In 2010, a Chinese telecommunications firm transmitted erroneous routing information for 37,000 computer networks, which misrouted some Internet traffic through China for 20 minutes. The attack exposed data from 8,000 U.S. networks, 1,100 Australian networks, and 230 French networks.[19]

Chinese cyber tactics

The People's Republic of China (PRC) is home to 1.35 billion people, or more than four times the population of the United States. Therefore, China often has the ability to overwhelm cyber defenses with quantity over quality, just as it did in the Korean War and as it might do in any other type of conflict.

The Chinese malware that FireEye researchers have analyzed is not the most advanced or creative. But in many circumstances, it has been no less effective. China employs brute-force attacks that are often the most inexpensive way to accomplish its objectives. The attacks succeed due to the sheer volume of attacks, the prevalence and persistence of vulnerabilities in modern networks, and a seeming indifference on the part of the cybercriminals to being caught.

[17] Report: Plans for Australia spy HQ hacked by China », (28 mai 2013) Associated Press.
[18] « Tracking GhostNet: Investigating a Cyber Espionage Network », (29 mars 2009) Information Warfare Monitor.
[19] Vijayan, J. (18 novembre 2010) « Update: Report sounds alarm on China's rerouting of U.S. Internet traffic », Computerworld.
[20] Sanger, D., Barboza, D. et Perlroth, N. (18 février 2013) « Chinese Army Unit is seen as tied to Hacking against U.S. », The New York Times.
[21] Pidathala, V., Kindlund, D. et Haq, T. (1er février 2013) « Operation Beebus », FireEye.

The "Comment Crew,"[20] a prominent example of a Chinese cyber threat actor, is believed to be a contractor to the PRC government. The Comment Crew is behind many noteworthy attacks, including Operation Beebus, which targets U.S. aerospace and defense industries.[21]

One important characteristic of the Comment Crew—which puts it definitively in the category of an advanced persistent threat, or APT—is that it is a bureaucracy. In-depth analysis reveals a small group of creative and strategic thinkers at the top. One layer down, a larger group of specialists design and produce malware in an industrial fashion. At the bottom are the foot soldiers—brute-force hackers who execute orders and wage extended cyber attack campaigns, from network reconnaissance to spear phishing to data exfiltration. The Comment Crew is so large, in fact, that when the Federal Bureau of Investigation (FBI) decoded one of the group's stolen caches of information, if printed out, it would have created a stack of paper taller than a set of encyclopedias.[22]

Such a large bureaucracy helps to explain sometimes-incongruous cybercriminal behavior. A given piece of malware, for example, may have been written by an expert but incorrectly used later by an inexperienced foot soldier (such as a poorly written spear phishing email). Understanding this cyber attack life cycle and its different stages can help cyber defenders recognize and foil an attack. In any large organization, some processes are less mature than others, and therefore easier to recognize.

Chinese cyber defense

In its own defense, Chinese officials contend that their country is also a target of cyber attacks. In 2006, the China Aerospace Science & Industry Corporation (CASIC) found spyware on its classified network.[23] In 2007, the Chinese Ministry of State Security stated that foreign cybercriminals were stealing Chinese information, with 42 percent of attacks coming from Taiwan and 25 percent from the United States.[24] In 2009, Chinese Prime Minister Wen Jiabao announced that a cybercriminal from Taiwan had stolen his upcoming report to the National People's Congress.[25] In 2013, Edward Snowden, a former system administrator at the National Security Agency (NSA), published documents suggesting that the U.S. conducted cyber espionage against China;[26] and the Chinese Computer Emergency Response Team (CERT) stated that it possessed "mountains of data" on cyber attacks by the U.S.[27]

[20] Sanger, D., Barboza, D. & Perlroth, N. (18 Feb 2013) "Chinese Army Unit is seen as tied to Hacking against U.S." The New York Times.
[21] Pidathala, V., Kindlund, D. & Haq, T. (1 Feb 2013) "Operation Beebus," FireEye.
[22] Riley, M. & Lawrence, D. (26 Jul 2012) "Hackers Linked to China's Army Seen From EU to D.C.," Bloomberg.
[23] "Significant Cyber Incidents Since 2006," Center for Strategic and International Studies.
[24] Ibid.
[25] Ibid.
[26] Rapoza, K. (22 June 2013) "U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press," Forbes.
[27] Hille, K. (5 Jun 2013) "China claims 'mountains of data' on cyber attacks by US," Financial Times.

North Korea—the upstart

North and South Korea remain locked in one of the most intractable conflicts on Earth. North Korea (supported by China) would seem to be stuck in a cyber Stone Age—especially relative to South Korea (supported by the U.S.)—has the fastest download speeds in the world[28] and will issue its students with computer tablets instead of books by 2015.[29] Even so, the Internet offers anyone, and any nation, an asymmetric way to gather intelligence and project national power in cyberspace—and North Korea appears to have acquired cyber attacks as a new weapon for its arsenal.

In 2009, North Korea launched its first major assault on South Korean and U.S. government websites. The attack did little damage, but the incident gained wide media exposure.[30] By 2013, however, the threat actors had matured. A group dubbed the "DarkSeoul Gang" was responsible for at least four years of high-profile attacks on South Korea. The group's attacks included a distributed denial-of-service (DDoS) attack and malicious code that wiped computer hard drives at banks, media, ISPs, telcos, and financial services companies—overwriting legitimate data with political messages. In the Korean conflict, such incidents often take place on dates of historical significance, including July 4, the U.S. Independence Day.[31] Suspected North Korean attacks on U.S. institutions include U.S. military elements based in South Korea, the U.S.-based Committee for Human Rights in North Korea, and even the White House.

North Korean defectors have described a burgeoning cyberwarfare department of 3,000 personnel, largely trained in China and Russia. The defectors stressed that North Korea has a growing fascinationwith cyber attacks as a cost-effective way to compete against its conventionally superior foes. They believe that North Korea is growing increasingly comfortable and confident in this new warfare domain, assessing that the Internet is not only vulnerable to attack but that this strategy can create psychological pressure on the West. Toward this end, North Korea has focused on disconnecting its important servers from the Internet, while building a dedicated "attack network."[32]

FireEye researchers have seen a heavy use of spear phishing and the construction of a "watering hole," in which an important website is hacked in the hope of compromising the computers of its subsequent visitors, who usually belong to a certain VIP-profile the attacker is targeting. Some North Korean attacks have begun to manipulate a victim's operating system settings and disable their anti-virus software—techniques that are normally characteristic of Russian cybercriminals. In other words, North Korean hackers may have learned from or have contracted support in Russia.

Apart from any possible disruption or destruction stemming from cyber attacks, computer network operations are an invaluable tool for collecting sensitive information, especially when it resides on government or think-tank networks normally inaccessible from the Internet. North Korea, China, and Russia are all naturally interested in collecting cyber intelligence that would increase their comparative advantage in classified information, diplomatic negotiating positions, or future policy changes.

[28] McDonald, M. (21 Feb 2011) "Home Internet May Get Even Faster in South Korea," The New York Times.
[29] Gobry, P-E. (5 JUL 2011) "South Korea Will Replace All Paper With Tablets In Schools By 2015," Business Insider.
[30] Choe Sang-Hun, C. & Markoff, J. (8 Jul 2009) "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," The New York Times.
[31] "Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War," (27 Jun 2013) Symantec.
[32] Fisher, M. (20 March 2013) "South Korea under cyber attack: Is North Korea secretly awesome at hacking?" The Washington Post.

At the same time, North Korea also asserts that it is a target of cyber attacks from South Korea and the U.S. In June 2013, when the North suffered a two-day outage of all of its in-country websites, its state news agency denounced "concentrated and persistent virus attacks," and proclaimed that the U.S. and South Korea "will have to take the responsibility for the whole consequences." The North noted that the attack took place in parallel with Key Resolve (joint U.S.-South Korean military exercises), but the U.S. Joint Chiefs of Staff denied any connection.[33]

India-Pakistan: old rivals, new tactics

A heavily fortified border separates India and Pakistan on the map. But the quiet, borderless nature of cyberspace means both sides are free to engage in cyber warfare—even during peacetime.

In 2009, India announced that Pakistani cybercriminals had placed malware on popular Indian music download sites as a clever, indirect way to compromise Indian systems.[34] In 2010, the "Pakistani Cyber Army" defaced and subsequently shut down the website of the Central Bureau of Investigation, India's top police agency.[35] In 2012, over 100 Indian government websites were compromised.[36]

Not to be outdone, in 2013, cybercriminals in India undertook "Operation Hangover," a large-scale Indian cyber espionage campaign that hit

Pakistani IT, mining, automotive, legal, engineering, food service, military, and financial services networks.[37] Although researchers could not definitively tie the attacks to India's government, many of the targets represented the country's national security interests.[38]

Association of Southeast Asian Nations (ASEAN): emerging economies as soft targets

Since at least 2010, many APTs (likely China-based) have targeted the governments, militaries, and businesses of ASEAN, the Southeast Asian geopolitical and economic group composed of Brunei, Burma (Myanmar), Cambodia, Indonesia, Laos, Malaysia, Philippines, Singapore, Thailand, and Vietnam. Although chances of any regional war erupting in the near term are low, a large volume of ongoing, regional cyber espionage activity is a constant. Targeted industries include telecommunications, transportation, oil and gas, banks, and think tanks. The usual motivation is to gain tactical or strategic advantage within the political, military, and economic domains.[39]

FireEye researchers are following numerous APT actors in this region, including BeeBus, Mirage, Check Command, Taidoor, Seinup, and Naikon. Their most common tactic is spear phishing, often using legitimate decoy documents that are related to the target's national economy or politics, or to regional events such as ASEAN summits, Asia-Pacific Economic Cooperation (APEC) summits, energy exploration, or military affairs.

[33] Herman, S. (15 Mar 2013) "North Korea Blames US, South for 'Cyber Attack'," Voice of America.
[34] "Significant Cyber Incidents Since 2006," Center for Strategic and International Studies.
[35] "India and Pakistan in cyber war," (4 Dec 2010) Al-Jazeera.
[36] Muncaster, P. (16 March 2012) "Hackers hit 112 Indian gov sites in three months," The Register.
[37] "Operation Hangover: Q&A on Attacks," (20 May 2013) Symantec.
[38] "Snorre Fagerland, et al. "Operation Hangover: Unveiling an Indian Cyberattack Infrastructure." May 2013.
[39] Finkle, J. (4 Aug 2011) "'State actor' behind slew of cyber attacks," Reuters.

FireEye believes that many of these regional economic organizations are attractive targets for APT campaigns because the information they possess is valuable and their level of cyber security awareness is low. Often, these organizations have inconsistent system administration, infrequent software patch management, poor policy control, or some combination of these issues. Thus, many of these networks are "low-hanging fruit" for attackers. And to make matters worse, compromised systems are used as staging grounds for further attacks on regional targets, by installing illicit command-and-control (CnC) servers, abusing legitimate email accounts, and disseminating stolen office documents as "bait."

Russia/Eastern Europe

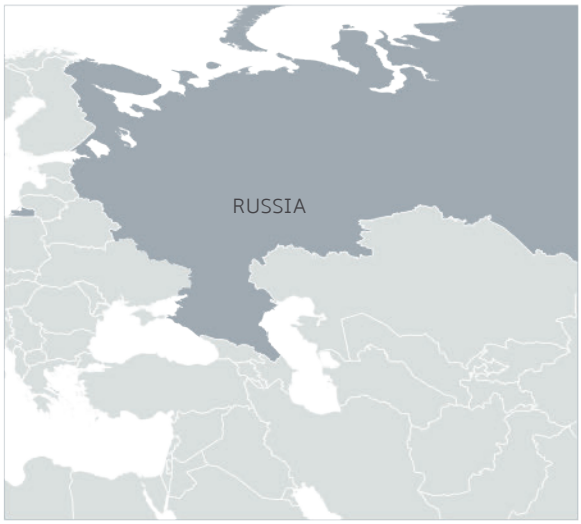
Russia—a little bit "too quiet?"

In 1939, Winston Churchill declared that Russia was a "riddle wrapped in a mystery inside an enigma …". Seven decades later, cyber defense researchers would say that not much has changed. Compared with the constant attacks detected from China, you can almost hear the snow falling on Red Square. One of the outstanding questions in cyber security today is: Where are the Russians? Perhaps they are simply great hackers. Maybe they have sufficient human intelligence. Whatever the reason, cyber defense analysts often look in vain for the traces of Russian cybercriminals. As a step toward finding some answers, however, consider the second half of Churchill's quote: "… but perhaps there is a key—that key is Russian national interest."[40] In other words, where there is smoke, there is usually fire.

In the mid-1990s, at the very dawn of the World Wide Web, Russia was engaged in a protracted struggle over the fate of Chechnya; the Chechens became pioneers in cyber propaganda, and the Russians became pioneers is shutting down their websites. In 1998, when Russian ally Serbia was under attack from NATO, pro-Serbian hackers jumped in the fray, targeting NATO with DoS attacks and at least twenty-five strains of virus-infected email. In 2007, Russia was the prime suspect in the most famous international cyber attack to date—the punitive DDoS on Estonia for moving a Soviet-era statue.[41]

In 2008, researchers uncovered clear evidence that computer network operations played a supporting role in Russian military advances during its invasion of Georgia.[42] Also in 2008, Russia was suspected in what U.S. Deputy Secretary of Defense William Lynn called the "most significant breach of U.S. military computers ever"—an attack on Central Command (CENTCOM), delivered through an infected USB drive.[43] In 2009, Russian cybercriminals were blamed in "Climategate," a breach of university research intended to undermine international negotiations on climate change mitigation.[44] In 2010, NATO and the European Union warned of increased Russian cyber attacks, while the FBI arrested and deported a possible Russian intelligence agent named Alexey Karetnikov, who had been working as a software tester at Microsoft.[45]

[40] "Winston Churchill," Wikiquote.
[41] Geers K. (2008) "Cyberspace and the Changing Nature of Warfare," Hakin9 E-Book, 19(3) No. 6; SC Magazine (27 AUG 08) 1-12.
[42] "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," (Aug 2009) U.S. Cyber Consequences Unit.
[43] Lynn, W.J. (2010) "Defending a New Domain: The Pentagon's Cyberstrategy," Foreign Affairs 89(5) 97-108.
[44] Stewart, W. & Delgado, M. (6 Dec 2009) "Were Russian security services behind the leak of 'Climategate' emails?" Daily Mail & "Global warning: New Climategate leaks," (23 Nov 2011) RT.
[45] Ustinova, A. (14 Jul 2010) "Microsoft Says 12th Alleged Russian Spy Was Employee," Bloomberg.



One ironic aspect of nation-state cyber attacks—especially in authoritarian countries—is that many of them are inward facing. In 2012, Russian security firm Kaspersky Lab announced the discovery of "Red October,"[46] a cyber attack campaign that spied on millions of citizens around the world, but chiefly within the former Soviet Union. Targets included embassies, research firms, military bases, energy providers, nuclear agencies, and critical infrastructure.[47] Similarly, in 2013, researchers found malware on millions of Android devices in Russia and in Russian-speaking countries. Either or both of these attacks could be partially explained as the Russian government keeping an eye on its own population, and that of neighboring countries.[48]

On the brighter side, as a step toward cyber détente, the U.S. and Russia in 2013 signed an agreement to build a cyber "hotline"—similar to that used for nuclear scares during the Cold War—to help defuse any computer-related crises in the future.[49] But, just to be on the safe side, Russia is taking the extreme cyber defense measure of buying old-fashioned typewriters,[50] and the Russian military is (like the U.S., China, and Israel) creating cyber warfare-focused units.[51]

Russian tactics

Though relatively quiet, Russia appears to be home to many of the most complex and advanced cyber attacks FireEye researchers have seen. More specifically, Russian exploit code can be significantly stealthier than its Chinese counterpart—which can also make it more worrisome. The "Red October" campaign, including its satellite software dubbed "Sputnik," is a prominent example of likely Russian malware.

TTP often includes the delivery of weaponized email attachments, though Russian cybercriminals appear to be adept at changing their attack patterns, exploits, and data exfiltration methods to evade detection. In fact, one telltale aspect of Russian hackers seems to be that, unlike the Chinese, they go to extraordinary lengths to hide their identities and objectives. FireEye analysts have even seen examples in which they have run "false-flag" cyber operations, designing their attack to appear as if it came from Asia.

[46] "The 'Red October' Campaign—An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies" (14 Jan 2013) GReAT, Kaspersky Lab.
[47] Lee, D. (14 Jan 2013) "'Red October'" cyber-attack found by Russian researchers," BBC News
[48] Jackson Higgins, K. (3 Aug 2013) "Anatomy of a Russian Cybercrime Ecosystem Targeting Android," Dark Reading.
[49] Gallagher, S. (18 Jun 2013) "US, Russia to install 'cyber-hotline' to prevent accidental cyberwar," Ars Technica.
[50] Ingersoll, G. (11 Jul 2013) "Russia Turns to Typewriters to Protect against Cyber Espionage," Business Insider.
[51] Gorshenin, V. (29 Aug 2013) "Russia to create cyber-warfare units," Pravda
.

Reconnaissance	Likely HUMINT Sources
Weaponization	Malicious DOC/XLS File Formats
Delivery	Weaponized Email Attachments
Exploitation	0-Day Application Vulnerabilities
Installation	Feature Rich RAT with Encrypted Modules
Command and Control (C2)	HTTP with Custom Embedded E ncoding / Encryption
Actions on Objectives	Intelligence Gathering (Govt. Focused)
TTP Exemplars	Red October

Table 2: Characteristics of Russian cyber attacks

One further problem for cyber defense researchers is that some Russian back doors into compromised systems are hard to distinguish from advanced cybercriminal break-ins.

Middle East

As a region, the Middle East may not possess the arsenal of zero-day exploits available in Russia, or the brute-force numbers of China. Therefore, some Middle Eastern hackers may have to rely on cyber tactics that emphasize novelty, creativity, and deception.

For example, the 2012 Mahdi campaign, which infected targets in the Middle East, used malicious Word documents, PowerPoint files, and PDFs to infect targets. That approach is similar to many other attackers. But these attacks were accompanied by some imaginative elements such as games, attractive images, and custom animations specifically designed to aid in the attack.

Not only did they trick users into executing commands to install malicious code, but they also distracted users from seeing malware-related warning messages. Furthermore, Mahdi attacks were tailored to specific target audiences—for example by offering variations of games unique to each organization. Such pinpoint strikes rely on prior reconnaissance, help to evade cyber defense behavioral-detection mechanisms, and dramatically increase the odds of compromise. So in the Middle East, the relative sophistication of an attack may be calculated less in the technology, and more in the clever ways in which malware is delivered and installed on a target network.

Reconnaissance	Regional Mailing Lists, Conferences
Weaponization	Malicious PPT/PPS Files
Delivery	Weaponized Email Attachments
Exploitation	Social Engineering Mouse Clicks on Screen
Installation	Primitive Collection of Custom Tools / RAT (Requires Operator For Lateral Movement)
Command and Control (C2)	Plain HTTP; Hiding in Plain Sight
Actions on Objectives	Intelligence Gathering (Middle East Focused), Denial of Service
TTP Exemplars	Madi, LV

Table 3: Characteristics of Middle Eastern cyber attacks

Iran: a "hot" cyber war

Wherever significant activity erupts in the real world (including crime, espionage, and warfare), parallel activity unfolds in cyberspace. It is therefore unsurprising that Iran—which has tense international relations and is on the verge of acquiring a nuclear bomb—has also experienced the most sophisticated cyber attacks to date.

In 2010, Stuxnet was a "cyber missile" of sorts designed with painstaking precision to burrow deep into Iran's nuclear program and destroy physical infrastructure. To some degree, this piece of software replaced a squadron of fighter aircraft that would have violated foreign airspace, dropped laser-guided bombs, and left a smoking crater in the Earth's surface.[52] Beyond Stuxnet, other advanced espionage attacks have worried security experts, including Duqu, Flame, and Gauss, which all may have come from the same threat actor.[53] And even amateurs are successfully targeting Iran; although the "Mahdi" malware is by comparison far less sophisticated than Stuxnet and its cousins, Mahdi has still managed to compromise engineering firms, government agencies, financial services firms, and academia throughout the Middle East.[54].

[52] Sanger, D. Confront and Conceal. (New York: 2012) pp. 188-225.
[53] Boldizsár Bencsáth. "Duqu, Flame, Gauss: Followers of Stuxnet," BME CrySyS Lab, RSA 2012.
[54] Simonite, T. (31 Aug 2012) "Bungling Cyber Spy Stalks Iran," MIT Technology Review.

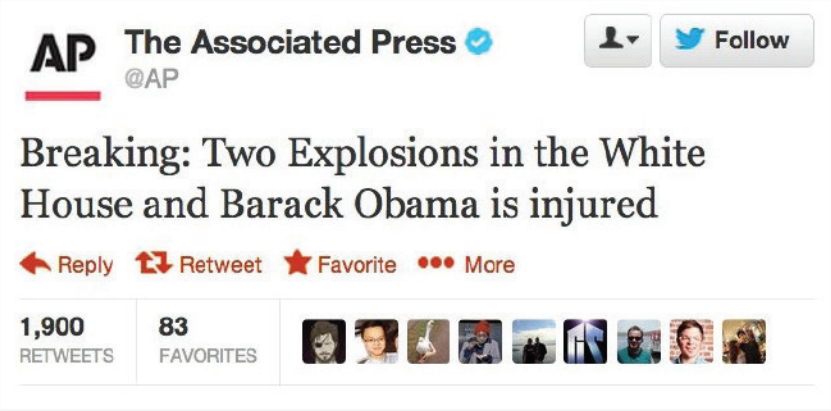
So how does anyone, including a nation-state, respond to a cyber attack? Does the counter-strike remain within the cyber realm, or can it come in the form of a traditional military (or terrorist) assault? In 2012, Iran appears to have chosen the first option. A hacker group called the "Cutting Sword of Justice" used the "Shamoon" virus to attack the Saudi Arabian national oil company Aramco, deleting data on three-quarters of Aramco's corporate PCs (including documents, spreadsheets, e-mails, and files) and replacing them with an image of a burning American flag.[55] And over the past year, another group called Izz ad-Din al-Qassam launched "Operation Ababil," a series of DDoS attacks against many U.S. financial institutions including the New York Stock Exchange.[56]

Other examples of cyber attacks abound. In 2009, the plans for a new U.S. Marine Corps 1 presidential helicopter were found on a file-sharing network in Iran.[57] In 2010, the "Iranian Cyber Army" disrupted Twitter and the Chinese search engine Baidu, redirecting users to Iranian political messages.[58] In 2011, Iranian attackers compromised a Dutch digital certificate authority, after which it issued more than 500 fraudulent certificates for major companies and government agencies.[59] In 2012, Iran disrupted the BBC's Persian Language Service, and University of Toronto researchers reported that some versions of the Simurgh "proxy" software (which is popular in countries like Iran and anonymizes Internet traffic) also installed a Trojan that collected usernames and keystrokes, sending them to a likely intelligence collection site.[60] Finally, in 2013 the Wall Street Journal reported that Iranian actors had increased their efforts to compromise U.S. critical infrastructure.[61]

Syria: what is the Syrian Electronic Army?

Syria is in the midst of a civil war, so researchers have a lot of cyber activity to analyze. The most prominent hacker group by far is the Syrian Electronic Army (SEA), which is loyal to Syrian President Bashar al-Assad. SEA has conducted DDoS attacks, phishing, pro-Assad defacements, and spamming campaigns against governments, online services, and media that are perceived to be hostile to the Syrian government. SEA has hacked Al-Jazeera, Anonymous, Associated Press (AP), BBC, Daily Telegraph, Financial Times, Guardian, Human Rights Watch, National Public Radio, The New York Times, Twitter, and more.[62] Its most famous exploit was a hoax announcement using AP's Twitter account that the White House was bombed and President Obama injured—after which stock markets briefly dipped to the tune of $200 billion.[63].

[55] Perlroth, N. (23 Oct 2012) "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," The New York Times.
[56] Walker, D. (8 Mar 2013) "Hacktivists plan to resume DDoS campaign against U.S. banks," SC Magazine.
[57] Borak, D. (3 Mar 2009) "Source in Iran views Marine One blueprints," Marine Corps Times.
[58] Wai-yin Kwok, V. (13 Jan 2010) "Baidu Hijacked By Cyber Army," Forbes.
[59] Charette, R. (9 Sep 2011) "DigiNotar Certificate Authority Breach Crashes e-Government in the Netherlands," IEEE Spectrum.
[60] "Iranian anti-censorship software 'Simurgh' circulated with malicious backdoor," (25 May 2012) Citizenlab.
[61] Gorman, S. & Yadron, D. (23 May 2013) "Iran Hacks Energy Firms, U.S. Says," Wall Street Journal.
[62] Fisher, M. & Keller, J. (31 Aug 2011) "Syria's Digital Counter-Revolutionaries." The Atlantic; "Syrian Electronic Army," (accessed 25 July, 2013) Wikipedia.
[63] Manzoor, S. (25 July, 2013) "Slaves to the algorithm: Are stock market math geniuses, or quants, a force for good?" The Sunday Telegraph.



In the month of July 2013 alone, SEA compromised three widely used online communications websites: Truecaller (the world's largest telephone directory),[64] Tango (a video and text messaging service),[65] and Viber (a free online calling and messaging application).[66] These types of compromises are significant because they can give Syrian intelligence access to the communications of millions of people, including political activists within Syria who might then be targeted for espionage, intimidation, and arrest.

To compromise its targets, the SEA often sends socially engineered, spear-phishing emails to lure opposition activists into opening fraudulent, weaponized, and malicious documents. If the recipient falls for the scam, Trojan horse, remote access tool (RAT) software is installed on the victim's computer that can give the attacker keystrokes, screenshots, microphone and webcam recordings, stolen documents, and passwords. And of course, the SEA likely sends all of this information to a computer address lying within Syrian government-controlled Internet Protocol (IP) space for intelligence collection and review.[67]

Israel: old conflict, new tactics

Even during the Cold War, the Arab-Israeli conflict saw many hot wars, and it was often the testing ground for new military weapons and tactics. Nothing has changed in the Internet era. Since at least 2000, pro-Israeli hackers have targeted sites of political and military significance in the Middle East.[68] In 2007, Israel reportedly disrupted Syrian air defense networks via cyber attack (with some collateral damage to its own domestic networks) to facilitate the Israeli Air Force's destruction of an alleged Syrian nuclear facility.[69]

[64] Khare, A. (19 July 2013) "Syrian Electronic Army Hacks Truecaller Database, Gains Access Codes to Social Media Accounts." iDigital Times.
[65] Kastrenakes, J. (22 July 2013) "Syrian Electronic Army alleges stealing 'millions' of phone numbers from chat app Tango." The Verge; Albanesius, C. (23 July 2013) "Tango Messaging App Targeted by Syrian Electronic Army." PCMag.
[66] Ashford, W. (24 July 2013) "Syrian hacktvists hit second mobile app in a week." Computer Weekly.
[67] Tsukayama, H. (28 Aug 2013) "Attacks like the one against the New York Times should put consumers on alert," The Washington Post.
[68] Geers K. (2008) "Cyberspace and the Changing Nature of Warfare," Hakin9 E-Book, 19(3) No. 6; SC Magazine (27 AUG 08) 1-12.
[69] Carroll, W. (26 Nov 2007) "Israel's Cyber Shot at Syria," Defense Tech.

But as an advanced industrial nation, Israel also depends on information technology. The nation has proven to be vulnerable to cyber attacks, which often target the Israeli economy. In 2009, during Israel's military operation in Gaza, hackers briefly paralyzed many government sites with a DDoS attack from at least 500,000 computers. The 2009 attack consisted of four independent waves, each stronger than the last, peaking at 15 million junk mail deliveries per second. The Israeli "Home Front Command" website, which plays a key role in national defense communications with the public, was down for three hours. Due to technical similarities with the 2008 cyber attack on Georgia during its war with Russia, Israeli officials surmised that the attack itself might have been carried out by a criminal organization in the former Soviet Union, and paid for by Hamas or Hezbollah.[70]

Often, the trouble with cyber attacks is that they do not need to be highly sophisticated to succeed, even against security-conscious Israel. In 2012, the ineptly written[71] "Mahdi" malware compromised at least 54 targets in Israel.[72] Last but not least, in 2013, the Iranian media reported that the Syrian army had carried out a cyber attack against the water supply of the Israeli city of Haifa. Prof. Isaac Ben-Israel, a cyber security adviser to Prime Minister Benjamin Netanyahu, said that the report was false, but added that cyber attacks on critical infrastructures pose a "real and present threat" to Israel.[73]

The West

United States

Analysts believe that the U.S. has conducted the most highly engineered cyber attacks to date, including Stuxnet,74 Duqu, Flame, and Gauss.75 This family of malware is unparalleled in its complexity and targeting. Stuxnet in particular was developed with a singular goal (to disrupt Iranian nuclear enrichment) that was both narrowly focused and capable of yielding strategic gains in the international arena. In contrast to computer worms such as Slammer and Code Red, Stuxnet did not seek to compromise as many computers as possible, but as few as possible. Even more amazing, its malicious behavior was concealed under a veneer of apparently legitimate operational data—but ultimately, the malware destroyed Iranian centrifuges.

This family of malware was exquisitely designed. For example, its payload can arrive at its destination encrypted—and become decrypted and installed only on a target device. This helps the malware to evade the prying eyes of cyber defenders, making discovering and reverse engineering the malware much more difficult.

Ironically, this family of malware could be a paragon of over-engineering. For example, it not only uses multiple zero-day exploits, but also world-first computational achievements such as a

[70] Pfeffer, A. (15 Jun 2009) "Israel suffered massive cyber attack during Gaza offensive," Haaretz.
[71] Simonite, T. (31 Aug 2012) "Bungling Cyber Spy Stalks Iran," MIT Technology Review.
[72] Zetter, K. (17 Jul 2012) "Mahdi, the Messiah, Found Infecting Systems in Iran, Israel," WIRED.
[73] Yagna, Y. (26 May 2013) "Ex-General denies statements regarding Syrian cyber attack," Haaretz.
[74] Sanger, D. Confront and Conceal. (New York: 2012) pp. 188-225.
[75] Boldizsár Bencsáth. "Duqu, Flame, Gauss: Followers of Stuxnet," BME CrySyS Lab, RSA 2012.
[76] Goodin, Dan (7 Jun 2012) "Crypto breakthrough shows Flame was designed by world-class scientists," Ars Technica.

Reconnaissance	Likely HUMINT Sources
Weaponization	Auto Infected Removable Media
Delivery	USB Removable Media
Exploitation	Social Engineering USB Media Use
Installation	Well-Crafted, Targeted (Crypto-Keyed) Worm (No Operator Required; Auto-Lateral Movement)
Command and Control (C2)	Strategic One-Time Use C2 Nodes; Full SSL Crypto
Actions on Objectives	Intelligence Gathering / Subtle System Disruption (Middle East Focused)
TTP Exemplars	Stuxnet, Flame, Duqu, Gauss

Table 4: Characteristics of Western cyber attacks

forced cryptographic "hash collision."76 In the case of Iran (which is currently subject to a trade embargo that restricts its acquisition of high technology), it is doubtful whether Iranian software is up-to-date or properly configured. So the authors of Stuxnet could likely have used more conventional computer exploits and still succeeded.

One possible telling aspect of U.S. cyber attacks: they require such a high level of financial investment, technical sophistication, and legal oversight that they will stand out from the crowd. On the last point, Richard Clarke, who served three U.S. Presidents as a senior counterterrorism official, argued that Stuxnet was a U.S. operation because "it very much had the feel to it of having been written by or governed by a team of Washington lawyers."[77] Finally, the amount of work involved in these operations suggests the participation of an enormous defense contractor base, with different companies specializing in particular aspects of a large and complex undertaking.

On the downside (and similar to the Israeli case), all advanced industrial economies are vulnerable to cyber counterattack. In 2008, a CIA official informed a conference of critical infrastructure providers that unknown cybercriminals, on multiple occasions, had been able to disrupt the power supply in various foreign cities.[78] In the military domain, Iraqi insurgents used $26 off-the-shelf software to intercept live video feeds from U.S. Predator drones, likely giving them the ability to monitor and evade U.S. military operations.[79] In the economic sphere, the U.S.-based International Monetary Fund (IMF) fell victim to a phishing attack in 2011 that was described as a "very major breach."[80]

Thus, while cyber attacks are relatively a new phenomenon, they represent a growing national security challenge. As part of a broader effort to mitigate the threat, President Obama signed a directive in 2013 that the U.S. should aid allies who come under foreign cyber attack.[81]

[77] Rosenbaum, R. (Apr 2012) "Richard Clarke on Who Was Behind the Stuxnet Attack," Smithsonian.
[78] Nakashima, E. & Mufson, S. (19 Jan 2008) "Hackers Have Attacked Foreign Utilities, CIA Analyst Says," Washington Post.
[79] Gorman, S., Dreazen, Y. & Cole, A. (17 Dec 2009) "Insurgents Hack U.S. Drones," Wall Street Journal.
[80] Sanger, D. & Markoff, J. (11 Jun 2011) "I.M.F. Reports Cyberattack Led to 'Very Major Breach'," New York Times.
[81] Shanker, T. & Sanger, D. (8 Jun 2013) "U.S. Helps Allies Trying to Battle Iranian Hackers," New York Times.

Europe

No prominent examples have been discovered of the European Union (EU) or the North Atlantic Treaty Organization (NATO) conducting their own offensive cyber attacks. On the contrary, their leaders have so far foresworn them.82 But many examples reveal European networks getting hacked from other parts of the world, particularly China and Russia.

Within government, cyber attacks on the British Foreign Ministry evaded network defenses in 2010 by pretending to come from the White House.[83] In 2011, German Police found that servers used to locate serious criminals and terrorism suspects had been penetrated, initially via a phishing attack.[84] Also in 2011, European Commission officials were targeted at an Internet Governance Forum (IGF) in Azerbaijan.[85]

In the military sphere, in 2009, French Navy planes were grounded following an infection by the Conficker worm.86 In 2012, the UK admitted that cybercriminals had penetrated its classified Ministry of Defense networks.[87]

In business, the European Union's carbon trading market was breached in 2011, resulting in the theft of more than $7 million in credits, forcing the market to shut down temporarily.88 In 2012, the European Aeronautic Defence and Space Company (EADS) and German steelmaker ThyssenKrupp fell victim to major attacks by Chinese cybercriminals.[89]

Security professionals should particularly be on the lookout for APT cyber threats just before and during international negotiations. In 2011 alone, the European Commission complained of widespread hacking before an EU summit,[90] the French government was compromised prior to a G-20 meeting,[91] and at least 10 Norwegian defense and energy companies were breached during large-scale contract negotiations, via phishing that was specifically tailored to each company.[92]

[82] Leyden, J. (6 June 2012) "Relax hackers! NATO has no cyber-attack plans—top brass," The Register.
[83] Arthur, C. (5 Feb 2011) "William Hague reveals hacker attack on Foreign Office in call for cyber rules," The Observer.
[84] "Hackers infiltrate German police and customs service computers," (18 July 2011) Infosecurity Magazine.
[85] Satter, R. (10 Nov 2012) "European Commission Officials Hacked At Internet Governance Forum," Huffington Post.
[86] Willsher, K. (7 Feb 2009) "French fighter planes grounded by computer virus," The Telegraph.
[87] Hopkins, N. (3 May 2012) "Hackers have breached top secret MoD systems, cyber-security chief admits," The Guardian.
[88] Krukowska, E. & Carr, M. (20 Jan 2011), "EU Carbon Trading Declines After Alleged Hacking Suspends Spot Market," Bloomberg.
[89] Rochford, O. (24 Feb 2013) "European Space, Industrial Firms Breached in Cyber Attacks: Report," Security Week.
[90] "'Serious' cyber attack on EU bodies before summit," (23 Mar 2011) BBC.
[91] Charette, R. (8 Mar 2011) "'Spectacular' Cyber Attack Gains Access to France's G20 Files," IEEE Spectrum.
[92] Albanesius, C. (18 Nov 2011) "Norway Cyber Attack Targets Country's Oil, Gas Systems," PCMag.

Conclusion

World War Z told a story of idiosyncratic national behavior in response to a major international crisis. This report sought to highlight the same phenomenon in regard to the challenges posed by national cyber insecurity and international cyber attacks. Behind every incident is an agenda—and individual human beings—each unique and ultimately identifiable. The bigger the cyber campaign, the more data it generates for security researchers, and the more difficulty attackers will have remaining anonymous and hiding their agenda.

As for crystal balls: no one knows what the next cyber attack will look like. But considering recent trends, we can make a few educated guesses.

Here are five factors that could change the world's cyber security landscape in the near- to medium-term:

1. **Outage of national critical infrastructure:** we know that cyber attacks can disrupt government networks, but most current cases simply do not rise to the level of a national security threat. Stuxnet—and Iran's alleged retaliation against Saudi Aramco—has shifted the thinking on cyber war from theory to something closer to reality. But have we seen the limit of what cyber attacks can achieve, or could cybercriminals threaten public safety by downing a power grid or financial market?

2. **Cyber arms treaty:** if world leaders begin to view cyber attacks as more of a liability than an opportunity, they may join a cyber arms control regime or sign a non-aggression pact for cyberspace. However, arms control requires the ability to inspect for a prohibited item. President Reagan's favorite Russian proverb was **доверяй, но проверяй**, or "trust but verify." Given that a single USB stick can now hold billions of bits of information, verifying would be easier said than done.

3. **PRISM, freedom of speech, and privacy:** we are still at the dawn of the Internet era, and this conversation has only just begun. It encompasses Daniel Ellsberg, Chelsea Manning, and Edward Snowden, as well as the Declaration of Independence, Enigma, and The Onion Router (TOR). Today, politicians, spooks, and hippies are all aware of a critical debate on the horizon—just how much online privacy should we have?

4. **New actors on the cyber stage:** the revolutionary nature of computers and the amplification power of networks are not exclusive to the world's largest nations. Iran, Syria, North Korea, and even non-state actors such as Anonymous have employed cyber attacks as a way to conduct diplomacy and wage war by other means. Researchers have little reason to think that other governments are not active in this domain. Possible candidates could be:

   a. Poland: it was the Poles who first broke the German Enigma cipher—way back in 1932! Today, with programming talent and well-known rivalry with Russia, it is a possibility.

   b. Brazil: Home to some of the world's most prolific cybercriminals, will Brazil's government, be angry about recent revelations of U.S. cyber spying, harness this talent for geopolitical ends?

   c. **Taiwan:** with constant cyber attacks emanating from Mainland China, Taipei may have little choice but to react.

5. **Stronger focus on evasion:** as we have seen, some nation-states know how to launch stealthy cyber attacks. But as the discipline of cyber defense matures, and as public awareness of the World War C phenomenon grows, some "noisy" cyber attackers such as China may be forced to raise their game by trying to fly under a more finely tuned radar.

The analysis and conclusions drawn in this paper are conjectural. Cyber security, cyber espionage, and cyber war are new and rapidly evolving concepts. Furthermore, most computer network operations are shrouded in secrecy. Deception is a given.

"A cyber attack, viewed outside of its geopolitical context, allows very little legal maneuvering room for the defending state," said Prof. Thomas Wingfield of the Marshall Center, in a recent email interview with FireEye. "False flag operations and the very nature of the Internet make tactical attribution a losing game."

But Wingfield adds that strategic attribution—fusing all sources of intelligence on a potential threat—allows a much higher level of confidence and more options for government decision makers. "And strategic attribution begins and ends with geopolitical analysis," he said. With this in mind, we hope that an awareness of this World War C dynamic helps cyber security professionals better understand, identify, and combat cyber attacks in the future.

About FireEye

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors, including Web, email, and files and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 1,100 customers across more than 40 countries, including over 100 of the Fortune 500.

For more information on next-generation threat protection, visit www.FireEye.com.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**

FireEye