DEFENSE DOSSIER

AUGUST 2012 ***ISSUE 4***

American Foreign Policy Council

DEFENSE DOSSIER

AUGUST 2012 **ISSUE 4**

American Foreign Policy Council

LETTER FROM THE EDITORS

Welcome to the August 2012 issue of the *Defense Dossier*, the e-journal of the American Foreign Policy Council. In this issue, we focus on the state of the American policy debate regarding cyber threats to U.S. national security.

Over the past several years, both state and non-state actors have demonstrated the ability to maliciously attack other countries' electronic infrastructure through cyber attacks. The U.S. Department of Defense computer systems have been hacked by foreign intruders, Russia has attacked Georgian and Estonian computer systems, and the Chinese have penetrated private sector U.S. defense firms. It is imperative that Congress and the White House move decisively to ensure not only that resources are in place to counter the mounting cyber threats confronting the United States, but that there is a clearly defined plan for oversight and response to cyber crimes and attacks.

With these goals in mind, AFPC hosted a conference on Capitol Hill this summer examining current and threats to U.S. national security and the state of the U.S. policy response to them. The articles in this *Defense Dossier* are drawn from the presentations featured at that event, which took place on July 19, 2012 in the Rayburn House Office Building of the U.S. House of Representatives. We would like to extend a special thanks to Congressman Michael McCaul (R-TX-10), who provided the conference keynote address, for the important role he plays in highlighting the cyber threats to U.S. national security and pushing forward legislation to counter those threats.

Sincerely,

Ilan Berman
Chief Editor

Rich Harrison
Managing Editor

ASSESSING THE CHINESE CYBER THREAT

By Larry Wortzel

China's government and Communist Party (CCP) use cyber operations for various purposes: to gather economic intelligence, for state intelligence operations, and to spy on people and control the flow of information. Computer network operations also have supported China's efforts to monitor foreign governments and activities outside China that the CCP considers a threat to its own control. Computer network operations also now are part of China's military planning.

The Communist Party and the People's Liberation Army (PLA) are focused on developing a world class military which would replace the United States as the leading security power in Asia. China's interpretation of regional security, however, means that other countries are coerced into acceding to China's vast claims in the South and East China Seas and to Beijing's threats to use force against Taiwan. PLA leaders want to dissuade the United States from conducting surveillance operations near China's coast, hinder access to the region by U.S. forces, and deny U.S. naval and air forces the ability to operate freely within about 1,700 kilometers of China. This is part of what the PLA terms a "counter-intervention" strategy.

China's military literature identifies cyber-attacks, combined with the ability to degrade U.S. satellites and surveillance assets, as a special weapon that can help it prevent the U.S. military from operating during or intervening in any conflict in the Western Pacific. As a result, cyber warfare and space warfare have become fully integrated elements of China's military operations planning. The PLA has developed doctrine and exercised an integrated information warfare capability that can defend military and civilian computer networks while seizing control of an adversary's information systems in a conflict.

Additionally, as the U.S. China Economic and Security Review Commission has documented, the PLA, the Ministry of State Security, and other state-related entities China have engaged in a massive effort to support peacetime computer network exploitation as a cornerstone of intelligence collection operations supporting national strategic goals.[1]

Stealing secrets

China's computer espionage has mined rich veins of information that previously were

Dr. Larry M. Wortzel *is a retired U.S. Army colonel. He served as director of the strategic Studies Institute at the U.S. Army War College and, after retirement, as Asian studies director and vice president at The Heritage Foundation. Since 2001, he has been a commissioner on the U.S.-China Economic and Security Review Commission, which he chaired for two years. This article is drawn from Wortzel's new book,* The Dragon Extends its Reach: Chinese Military Power Goes Global*, (forthcoming in 2013 from Potomac Books).*

inaccessible or which could be extracted only in small amounts with human intelligence operations. In two reports for the Commission, the Northrop Grumman Corporation provided evidence of how China is using computer espionage to support its modernization goals.[2] China's military intelligence collection and cyber reconnaissance infrastructure also supports a coordinated effort to combine civilian and military cyber programs and improve both offensive and defensive capabilities. Mark Stokes and his colleagues at the Project 2049 Institute, a think tank based in Arlington, Virginia, documented how the PLA General Staff Department (GSD) Third Department and Fourth Department are organized and structured to systematically penetrate communications and computer systems, extract information and exploit that information.[3]

China's military literature identifies cyber-attacks, combined with the ability to degrade U.S. satellites and surveillance assets, as a special weapon that can help it prevent the U.S. military from operating during or intervening in any conflict in the Western Pacific.

China has a national policy of espionage in cyberspace and is "the world's most active and persistent practitioner of cyber espionage today" according to Mike McConnell, former Director of National Intelligence, Michael Chertoff, former Secretary of Homeland Security; and William Lynn, former Deputy Secretary of Defense. In a January 2012 *Wall Street Journal* opinion piece, these former officials point out that "it is more efficient for the Chinese to steal innovations and intellectual property than to incur the cost and time of creating their own."[4] In addition to engaging in economic espionage, the U.S. National Counterintelligence Executive has documented intrusions from China into the computer systems of Congress and the U.S. government, global oil and energy companies, Google's networks, and the networks of U.S. Fortune 500 manufacturing corporations.[5] Some of these penetrations are aimed at acquiring the details on U.S. mergers and acquisitions, and related pricing and financial data.

Cyber intruders tied to China apparently have managed to gather "several terabytes of data related to design and electronics systems" of the F-35 Lightning II fighter.[6] Defense contractors such as the Lockheed Martin Corporation, Northrop Grumman Corporation, and British Aerospace and Engineering reportedly all have experienced penetrations from hackers based in China in the past three years.

China's cyber infrastructure

Cyber operations are a massive effort in China. The GSD Third Department is responsible for monitoring communications, communications security, computer network exploitation, and cyber security for the PLA. The Third Department has three research institutes of its own and four separate information centers. Additionally, Project 2049 documents twelve operational bureaus that have a strategic mission with regional or functional orientations to monitor

communications by phone, radio, satellite or computer.[7]

To support the PLA's seven military regional commands, the Third Department has another seventeen or so technical reconnaissance bureaus (TRBs). TRBs support theater-level operations in China's military regions as well as the PLA Air Force, Navy, and Second Artillery Force (the strategic rocket forces). Beijing, Jinan, Shenyang, and Guangzhou Military Regions each have one subordinate TRB, while Lanzhou, Chengdu, and Nanjing, each have two. The PLA Navy has two TRBs, the Air Force three, and the 2nd Artillery has one. Two of these TRBs focus directly on Taiwan.

The GSD Fourth Department, responsible for electronic countermeasures, electronic support measures, gathering electronic intelligence, and probably cyber attack works with the Third Department to penetrate information systems and assists in computer network exploitation. There also are militia units that have cyber-related missions for the PLA, and the People's Armed Police has its own technical reconnaissance unit.

A PLA strategy for orchestrating cyber-attacks with other forms of combat is "Integrated Network Electronic Warfare," or INEW. This strategy employs electronic warfare, psychological operations, deception, computer network operations, attacks on satellites, and kinetic strike, or traditional firepower warfare. Those of us who served in the military during the Cold War remember a Soviet military doctrine called Radio-electronic Combat, or REC. This doctrine combined electronic warfare, communications intercept, radio-direction finding, and strikes by artillery, helicopters, aircraft, missiles and rockets. The Soviet doctrine called for the capacity to degrade an adversary's combat capability by sixty percent at the outset of any conflict, in other words, at "zero-hour."

PLA INEW doctrine is Soviet Radio-electronic Combat on steroids. Chinese doctrine has added in computer network operations that would disrupt not only command and control, but also logistics systems, including in the adversary's homeland. China's INEW doctrine calls for operations to degrade an adversary's space-based sensor and communications systems. It also includes provisions for cyber and precision strikes on the adversary's bases, forces, and embarkation areas in the homeland.

But China's cyber strategy extends beyond the PLA and into the civil and commercial spheres. Several U.S. China Economic and Security Commission reports have expressed concerns about some of China's largest telecommunications firms, such as Huawei Shenzhen Technology Company, Zhongxing Telecom (ZTE) and Datang Telecom Technology, Ltd. These firms benefit from a network of state research institutes as well as government funding in programs that have affiliation or sponsorship of the People's Liberation Army. Starting with economic reforms in the 1980s, Chinese Communist Party leaders decided that a number of PRC companies would be promoted as "national champions" in various industrial sectors. The CCP and the government worked to brand the companies as major global businesses, in part to penetrate major western markets. In the telecommunications sector, Huawei and ZTE are two of the companies chosen by the CCP as "champions." One strategy to penetrate target markets that has been pursued by

Huawei is to hire former legislators and government officials from the targeted country as spokesmen, employees or lobbyists.

My concern, and that of many in the U.S. Congress, is the relationship between the senior executives and the board of Huawei (and other PRC "champion" companies) and the Chinese Communist Party. Among the relevant questions that need to be posed are: To what extent are these companies responsible for implementing PRC economic, foreign and security policies? Are senior executives or board members subject to CCP coercion? How do Communist Party cells and organizations function in the companies and their foreign subsidiaries? What means of secret communication does the CCP use for its Party cells in those companies? Thus far, Huawei has not revealed such information. Most recently, ZTE has been implicated in possible illegal diversion of U.S. telecommunications technology to Iran.[8]

"It is more efficient for the Chinese to steal innovations and intellectual property than to incur the cost and time of creating their own."

Telecommunications hardware and software can be built with remote access points or other features intended to facilitate penetrations, even of other equipment installed on the same network. These access points can be used to help gather information on, manipulate, or shut down a targeted network. Therefore, governments should have substantial concerns about the activities of Huawei and some other Chinese companies. Australia and the United States, for example, have blocked Huawei from large infrastructure deals on account of these concerns.

Penetrating U.S. strategic infrastructure

Computer network exploitation and cyber reconnaissance operations during peacetime support Chinese espionage, but they also identify the nodes in an information system or in an adversary's critical infrastructure for attack or take-over in a conflict. PLA writings on potential conflicts show how "Chinese commanders may elect to use deep access to critical U.S. networks carrying logistics and command and control data to collect highly valuable real-time intelligence or to corrupt the data without destroying the networks or hardware."[9]

The U.S. military's NIPRNET (Non-secure Internet Protocol Routing Network) is particularly vulnerable. This network carries much of the time phasing and force lists for deployments, personnel data, and communications with civilian defense contractors. An attack on the NIPRNET or the corruption of its data could affect the delivery of repair parts, ammunition, and aerial refueling, among other things.

The U.S. Department of Defense also has serious vulnerabilities in its telecommunications and weapons systems supply chains. Backdoors built into hardware or coded into firmware or software can be leveraged to gain unauthorized access to systems. If the U.S. government does not exercise strict control of the manufacturing channel it can be exposed to points of possible tampering.

In one noteworthy instance, as pointed out by Representative Frank R. Wolf in 2006, the U.S. State Department ordered computers clearly configured for use on a classified computer network and the supplier ordered them from a Chinese company. Ultimately, the installation and architecture needed to be revised.

More recently, the U.S. Army sourced a large number of computers from a Chinese company for use on installations critical to our NIPRNET-based logistics system and on installations that repair some of our most sensitive electronic sensors. Although Department of Defense officials believe that procurement policy provides that companies or equipment judged by the intelligence community to be a threat can be excluded from consideration, Army procurement and acquisition officials believe they only can exclude foreign firms if the information technology equipment is destined to go into weapons systems that are controlled under the United States Munitions List (Part 121 of the International Traffic in Arms Regulation or ITAR). The Office of the Secretary of Defense is still working to ensure that all services understand that the DOD can exclude foreign manufactured computer systems from going to a defense installation or on a system that is not ITAR controlled. It appears that the enterprise information architecture of the Department of Defense, indeed perhaps the whole U.S. government, should be a national security concern.

Taking Chinese cyberwar seriously

It is clear that cyber warfare is an active front in an ongoing intelligence war. Chinese military literature calls for cyber-attacks at the outset of any conflict. This means that the United States should have a clear policy that declares that attacks in cyber space are acts of war and that the U.S. may respond with force, not necessarily in the same domain. That is, a cyber-attack may generate a weapons strike and a state of war. ■

---

[1] See www.uscc.gov for USCC special reports on China's cyber operations and the Commission's Annual Reports to Congress.

[2] Brian Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," U.S.-China Economic and Security Review Commission (prepared by Northrop Grumman), October 9, 2009, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf; Brian Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage" U.S.-China Economic and Security Review Commission (prepared by Northrop Grumman), March 7, 2012, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf.

[3] Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure" Project 2049 Institute, November 11, 2011, http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf.

[4] Mike McConnell, Michael Chertoff and William Lynn, "China's Cyber Thievery Is National Policy—And Must Be Challenged," *Wall Street Journal*, January 27, 2012, http://online.wsj.com/article/SB10001424052970203718504577178832338032176.html.

[5] Office of the National Counterintelligence Executive, *Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011: Foreign Spies Stealing U.S. Economic Secrets in Cyberspace*, October 2011,

http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[6] Siobhan Gorman, August Cole and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, April 21, 2009, http://online.wsj.com/article/SB124027491029837401.html.

[7] Stokes, Lin and Hsiao, "The Chinese People's Liberation Army."

[8] Steve Stecklow and Melanie Lee, "FBI Probes China's ZTE Over Iran Tech Deals: Report," Reuters, July 13, 2012, http://www.reuters.com/article/2012/07/13/us-zte-fbi-idUSBRE86C00S201207130.

[9] Krekel, "Occupying the Information High Ground."

HOW RUSSIA HARNESSES CYBERWARFARE

By David J. Smith

Although most commentators on cyber threats to the United States appear fixated on China, we ignore Russia at our peril. In his 2010 book *Cyber War,* former White House cyber coordinator Richard Clarke said as much when he wrote that U.S. officials "do not rate China as the biggest threat to the US in cyberspace." Rather, experts have noted that "The Russians are definitely better, almost as good as we are."[1]

Other specialists concur. "Unlike China," Jeff Carr, the CEO of Taia Global, explains on his *Digital Dao* blog, "Russian cyber operations are rarely discovered, which is the true measure of a successful op."[2]

Never mind, for a moment, which country is number one and which is number two. Russia—its government and a motley crew of government-sponsored cyber-criminals and youth group members—has integrated cyber operations into its military doctrine and is conducting strategic espionage against the United States. Moreover, it spares no diplomatic effort in trying to forge a path forward for its nefarious activities while resisting efforts to do anything constructive in the international arena.

The drivers of Russian policy

To explain all this, it is first necessary to set out two points about Russia: 1) Russia is characterized by a unique nexus of government, business and crime; and 2) Russia takes a much broader approach to information operations than do most western countries.

Corruption is the dominant characteristic of the current Russian polity. And with systemic corruption come opportunities for collusion on just about everything. Rule of law flies out the window, replaced by personal relationships and payoffs. Laws are enforced arbitrarily—what matters is one's circle of friends. No one gets rich, no one succeeds, no one does anything big without at least the acquiescence of President Vladimir Putin's inner circle. And there is a *quid pro quo* for everything.

The second basic point is that Russia holds a broad concept of information warfare, which includes intelligence, counterintelligence, deceit, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, degradation of information systems

Amb. David J. Smith *is Director of the Potomac Institute Cyber Center. He has a 30 year career in international relations, including the US Air Force, Intelligence Community, Defense and State Departments, and both houses of Congress. From 1989 until the demise of the Soviet Union, he was US Ambassador at the US-Soviet Defense and Space talks. The above article is an excerpt from a future publication by Amb. Smith, and he retains the copyright to this work.*

and propaganda. Computers are among the many tools of Russian information warfare, which is carried out 24 hours a day, seven days a week, in war and in peace. Seen this way, distributed denial of service (DDoS) attacks, advanced exploitation techniques and *Russia Today* television are all related tools of information warfare.

This broad concept is woven into Russia's military strategy. Russia's way of war includes information warfare and it follows that information warfare against Russia will be considered warfare. The 2010 Russian military doctrine calls for "prior implementation of measures of informational warfare in order to achieve political objectives without the utilization of military forces."[3] The objective is war without tanks or, more likely, war with fewer tanks, especially at the initial stages.

U.S. officials "do not rate Russia as the biggest threat to the US in cyberspace." Rather, experts have noted that "The Russians are definitely better, almost as good as we are."

Russia's 2008 combined cyber and kinetic attack on Georgia was the first practical test of this doctrine. Although it was not fully successful, we must assume that the Russian military has studied the lessons learned, just as it has done for every other facet of its poor performance against Georgia.

The Russian war on Georgia also bears lessons for the United States. We must be mindful of relatively simple DDoS attacks conducted for political and military purposes, particularly against smaller allied countries upon which we depend.

However, we must also assume—given all the doctrinal attention paid to the subject—that Russia is honing far more sophisticated military cyber capabilities. Of course, roles and capabilities in this regard are harder to grasp through open source analysis. At least some indications are available, however. For example, Deputy Prime Minister Dmitry Rogozin recently said that Russia will soon form a military cyber command.[4] Whether hidden or open, the Russian military is likely endowed with the panoply of offensive and advanced exploitation capabilities.

The infrastructure of Russian cyberwar

At home, Russia also has a concept of information security very different from western countries. The September 2000 *Doctrine of Information Security of the Russian Federation*—published just eight months into Putin's presidency—sets forth three objectives.[5] The first Russia shares with just about every country in the world: to protect strategically important information. However, the second and third objectives set Russia apart, at least from democratic countries: to protect against deleterious foreign information and to inculcate in the people patriotism and values.

Another unique feature of the Russian approach is extensive reliance on youth groups such as the Kremlin-controlled *Nashi* and cyber-criminal syndicates such as the now invisible Russian Business Network (RBN). Until its apparent demise in 2008, RBN was involved in just about every nasty scheme imaginable—phishing, malware,

malicious code, DDoS attacks, child pornography and more. And do not imagine that this kind of organization has gone away—its principals are no doubt active somewhere else on the web.

There are two reasons why Russia sub-contracts some of its cyber work to youth groups and criminals. First, it is extremely cost-effective; imagine a reserve force that not only does not cost money, but actually makes money when not employed by the state. Second, use of kids and criminals compounds the attribution problem; even after extensive cyber forensics, attacks are not traced back to government computers. This is particularly confusing to many westerners who cannot imagine a government so intertwined with such people.

And there are plenty of well-trained people to carry out these activities. Russia is a typical extractive economy that still enjoys the benefits of the quite good Soviet educational system. Great wealth is concentrated in the hands of a few, while many people with training in math, science and computers look for work. The result is a thriving botnet-for-hire industry.

Botnets for hire went to work against Estonia in 2007. The Estonian government had decided to move the "Bronze Soldier of Tallinn" statue from the city center to a military cemetery. Ethnic Russians and Russia took this as an offense—or at least as an excuse for trouble. Russian politicians arrived in Estonia to rile things up and some Russian language websites offered instructions on which Estonian websites to attack and how to do it. For a week in late April and early May, simple DoS attacks were carried out, somewhat ineffectively. Then the professional botmasters went to work with DDoS attacks, threatening essential services and doing significant damage to the Estonian economy.

In 2008, it was Georgia's turn in the first ever combined kinetic and cyber-attack. Many of the same techniques and computers involved against Estonia a year earlier resurfaced against Georgia.

Exhibiting remarkable insight on the part of the perpetrators, defacement of Georgian government websites, particularly the president's website, began more than two weeks before the physical Russian invasion of Georgia. On the day the war started, sites such as stopgeorgia.ru sprang up with a list of sites to attack, instructions on how to do it and even an after-action report page. It is instructive that all this was ready to go—surveys, probing, registrations, and instructions—on day-one of the conflict.

An Internet blockade was traced to five autonomous systems, four in Russia and one in Turkey, all controlled by the criminal syndicate Russian Business Network. Then came fake news reports that dumped Trojans into the computer of anyone beguiled into clicking on a link. And there was a final large DDoS attack two weeks after the ceasefire. When one considers the forensic evidence, geopolitical situation, timing and the relationship between the government and the youth and criminal groups, it is not difficult to conclude that the Kremlin was behind it all.

Cyberwar against Russian democracy

Three years later, we learned that the Kremlin treats all enemies, foreign and

domestic, the same. In the spring of 2011, again with many of the same techniques and computers employed against Estonia and Georgia, DDoS attacks were directed against websites generally associated with opposition to the Putin government. On March 24th, the LiveJournal blog page of anti-corruption crusader Aleksey Navalny was attacked, followed two days later by an attack on his rospil.info, which tracks government procurement contracts.

If Navalny's nagging blogsite was insufficient provocation, the People's Freedom Party—led by Boris Nemtsov, Vladimir Milov, Mikhail Kasyanov and Vladimir Ryzhkov—was about to post its new report, *Putin. Corruption,* on LiveJournal. On April 4th, LiveJournal sustained a major DDoS attack. Maria Garnaeva of Kaspersky Lab blogged that at least two botnets were involved.[6] One of them was "Darkness," then a favorite of the Russian underworld.

In response, Nemtsov commented, "Hardly anyone could have done this other than the security services… LiveJournal is truly a territory of freedom and this is a preparation for parliamentary and presidential elections."[7]

Then it was the turn of the newspaper *Novaya Gazeta.* Its *Online Parliament of the Runet* had no doubt irked some folks in the Kremlin. Constituents of the blogosphere nominated candidates for the electronic parliament, followed by an online election. Then the elected members were to debate online issues that, in their view, the official government was skirting. On April 7th-8th, DDoS attacks were mounted on *Novaya Gazeta.*

Nemtsov was apparently correct that the March-April attacks were a dry run for the December 4th Duma elections. On the day of the elections, a number of websites generally associated with the opposition were taken down by DDoS attacks. However, the perpetrators apparently miscalculated the power of the Internet. They appear to have been obsessed with a site called kartanarusheniy.ru, which was an interactive map of election violations, sponsored by the election watchdog Golos, which receives funds from the National Endowment for Democracy. Kartanarusheniy itself was taken down, as were sites that linked to it or mentioned it. However, many other sites were untouched; indeed, one could read about the sites that were dark on the sites that remained up. It seems that a few DDoS attacks do not cow everybody as a few arrests and a beating or two used to do.

Social media and blogsites were very active right through the March 4th presidential election; however, the Kremlin's botmasters were apparently called off altogether. Another indication that the government controls them is the discipline with which they all desisted. Had they been truly independent patriotic hackers, one would have expected at least a few of them to have persisted in their online hijinks.

Russia's new normal

Today, the Kremlin is worried—worried about Arab Spring, London riots, unrest in the North Caucasus, likely attempts to subvert the 2014 Sochi Winter Olympics and, of course, the unprecedented social media-borne anti-Putin demonstrations across Russia.

Unsurprisingly, Russia's diplomatic activities on the cyber front reflect its policies on information warfare and information security. While steadfastly refusing to sign the *European Convention on Cybercrime,* a highly effective international approach to cyber security challenges, it joins China and a few others in plying proposals aimed at enhancing information security—that is, shielding autocratic states from the free flow of information across the Internet.

Meanwhile, Russia has undertaken a major effort at strategic cyber espionage against the United States. It is strategic in the sense that it is not just a government's spy agency trying to steal bits of classified information or an enterprise conducting industrial espionage. Rather, it is a concerted effort to steal American intellectual property to achieve a level technological development that Russia cannot achieve on its own. In this regard, it is worth repeating an October 2011 finding of the U.S. Counterintelligence Executive.

Motivated by Russia's high dependence on natural resources, the need to diversify its economy, and the belief that the global economic system is tilted toward US and other Western interests at the expense of Russia, Moscow's highly capable intelligence services are using HUMINT, cyber, and other operations to collect economic information and technology to support Russia's economic development and security.[8]

In sum, Russia—in its capabilities and its intent—presents a major cyber challenge to the United States. The only difference between it and China may be, as Jeff Carr points out, that it is seldom caught. And that, alone, may make it the number one cyber threat. ■

---

[1] As cited in Richard Clarke, *Cyber War: The Next Threat to National Security and What to do About It* (Ecco, 2010)

[2] Jeffrey Carr, "7 Reasons Why China Isn't the World's Biggest Cyber Threat (and Who Is)" *Digital Dao,* June 29, 2011, http://jeffreycarr.blogspot.com/2011/06/7-reasons-why-china-isnt-worlds-biggest.html.

[3] Security Council of the Russian Federation, "Voennaya Doctrina Rossiyskoi Federatsii," June 25, 2010, http://www.scrf.gov.ru/documents/33.html.

[4] "Russia Considering Cyber Security Command," RIA Novosti, March 21, 2012, http://en.rian.ru/russia/20120321/172301330.html.

[5] Russian Federation, Ministry of Foreign Affairs, *Information Security Doctrine of the Russian Federation,* September 9, 2000, http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument.

[6] Maria Garnaeva, "LiveJournal Under Attack," *Securelist,* April 6, 2011, http://www.securelist.com/en/blog/442/LiveJournal_under_attack.

[7] "Russian Bloggers Accuse Authorities of Cyberwar," Agence France-Presse, April 6, 2011, http://www.google.com/hostednews/afp/article/ALeqM5haQ7xYOW7niqLaPw6cEkFzO0Tozw.

[8] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace,* October 2011, 5, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

CYBERWAR AND IRANIAN STRATEGY

By Ilan Berman

In the evolving discourse regarding cybersecurity now visible in Washington, the Islamic Republic of Iran has generally gotten short shrift. Indeed, the Iranian regime—currently facing widening multilateral sanctions as a result of its nuclear ambitions, and grappling with an increasingly contentious domestic political scene—tends to be dismissed as neither a serious nor an imminent cyber threat to the United States.

Yet, for precisely those reasons, U.S. policymakers would do well to focus on the Iranian regime's cyberwarfare capabilities, as well as its growing ability to hold the homeland at risk. Doing so begins by understanding the nature of Iran's contemporary focus on cyberspace.

Iran versus the World-Wide Web

In a very real sense, the Iranian regime today can be said to be erecting an "electronic curtain" aimed at isolating its population from the World Wide Web. It is doing so through an array of concrete initiatives.

The most prominent of these is the creation of an alternative national intranet. Originally slated to go online in August 2012, this "halal" or "second" internet represents a more sophisticated alternative to filtering systems such as China's "Great Firewall." While those simply deny users access to proscribed sites, Iran's will reroute them to regime-approved search results, websites, and online content. By doing so, it will give Iranian authorities the power to create an Islamic Republic-compliant online reality for their citizens.

The Iranian government is also dedicating a new agency to monitor cyberspace. This "Supreme Council of Cyberspace," now in formation, will be headed by top officials from both Iran's intelligence apparatus and the Revolutionary Guards and tasked with "constant and comprehensive monitoring over the domestic and international cyberspace." Once operational, it will be able to issue sweeping decrees concerning the Internet that would have the full strength of law.[1]

This has been supplemented by draconian new rules and restrictions on Internet usage. Internet cafes, for example, are now mandated to record the personal information of customers—including vital data such as names, national identification numbers, and phone numbers—as well the installation of closed-circuit cameras to keep video logs of all customers accessing the World-Wide Web.[2] Onerous penalties for online content deemed inappropriate or subversive have been passed as well.

Finally, the Iranian regime has harnessed new

Ilan Berman *is the Vice President of the American Foreign Policy Council in Washington, D.C.*

technologies for monitoring, filtering, and limiting access. In this effort, Iran has been assisted by a number of foreign entities. Most notably, China's ZTE Corp. has partnered with the state-controlled Telecommunication Company of Iran (TCI) to implement advanced monitoring of the country's telecom sector.[3]

Iran's focus on constricting Internet freedom is understandable. The Iranian regime faces an array of domestic challenges to its authority. These include the so-called "Green Movement" which coalesced following the fraudulent reelection of Mahmoud Ahmadinejad to the Iranian presidency in June of 2009. That event galvanized an outpouring of popular discontent, which coalesced into a broad opposition front known as the "Green Movement." "Green Movement" activists relied heavily on social media—including Twitter, Facebook and other networking platforms—to organize their protests and activities. In response, the Iranian regime utilized information and communication technologies extensively in its suppression of the protests—and thereafter has invested heavily in capabilities aimed at controlling and restricting access to the World-Wide Web.[4]

Cybersecurity experts warn that, should the standoff over Iran's nuclear program precipitate a military conflict, Iran "might try to retaliate by attacking U.S infrastructure such as the power grid, trains, airlines, refineries."

An additional source of concern is the so-called "Arab Spring" which has swept over the Greater Middle East over the past year-and-a-half. So far, Iran has been spared the anti-establishment sentiment that has led to upheavals in Tunisia, Libya, Egypt and, most recently, Syria. But Iran's leaders are deeply worried about the possibility of anti-regime sentiment migrating to their country, and as a result have done their best to limit their population's exposure to such ideas via the media and Internet.

Quiet conflict over Iran's nuclear program

Over the past three years, the Iranian nuclear program has come under sustained and repeated cybernetic attack. To date, at least five distinct cyber worms targeting the Iranian nuclear program have been identified and isolated. These include Stuxnet, the malicious software that attacked Iran's centrifuge arrays between mid-2009 and late 2010; "Stars," a software script targeting execution files; DuQu, a successor to Stuxnet aimed at gaining remote access to Iran's nuclear systems; another piece of malware named Wiper, which attacked internal Internet communications; and, most recently, Flame, a cyber espionage virus.

And still more are on the horizon. In July of 2012, it was revealed that Iran has been attacked by a new cyberworm dubbed "Mahdi."[5] Although comparatively unsophisticated, "Mahdi"—unlike previous such attacks—appears to be of indigenous origin, suggesting that the Iranian regime now faces cyber enemies not only outside its borders, but within them as well.

The Iranian regime has begun a significant mobilization in response. It has launched an ambitious $1 billion governmental program to boost national cyber capabilities—an effort

that involves acquisition of new technologies, investments in cyber defense, and the creation of a new cadre of cyber experts.[6] It has also activated a "cyber army" of activists which, while nominally independent, carried out a series of attacks on sites and entities out of favor with the Iranian regime, including the social networking site Twitter, the Chinese search engine Baidu, and the websites of Iranian reformist elements.[7]

As these developments indicate, Iran appears increasingly to be moving from defense to offense in terms of how it thinks about cyberspace. Accordingly, in late July 2011, the hardline regime newspaper *Kayhan*, wrote in an editorial that America, which once saw cyberwarfare as its "exclusive capability," had severely underestimated the resilience of the Islamic Republic. The United States, the paper suggested, now needs to worry about "an unknown player somewhere in the world" attacking "a section of its critical infrastructure."[8]

This is not idle bluster; security professionals have taken note of Iranian efforts to probe segments of U.S. critical infrastructure, most notably the country's electrical sector.[9] Along those lines, cybersecurity experts warn that, should the standoff over Iran's nuclear program precipitate a military conflict, Iran "might try to retaliate by attacking U.S infrastructure such as the power grid, trains, airlines, refineries."[10]

Bracing for contact

There is an old axiom that the gravity of a threat is determined by both capability and intent, and this holds true for cyberwarfare as well. Today, Iran is not the greatest cyber threat arrayed against the United States. Indeed, while significant, Iranian capabilities are generally judged to be inferior to those of China and Russia—perhaps considerably so.[11] What Iran lacks in capability, however, it makes up for in intent. Politically, a cyber attack from Iran is significantly more likely than from either China or Russia, in light of the ongoing international impasse over its nuclear program.

It is not out of the question that the Iranian regime could independently initiate a cyber attack on the United States. Iran has grown significantly bolder in its foreign policy of late, and no longer can be relied upon to refrain from direct action in or against the U.S. homeland. As Director of National Intelligence James Clapper noted in his testimony before the Senate Select Committee on Intelligence this past January, "Iranian officials—probably including Supreme Leader Ali Khamenei—have changed their calculus and are now willing to conduct an attack in the United States."[12]

Far more probable, however, is the possibility of a development related to Iran's nuclear program serving as a trigger for some sort of attack in the cyber realm by the Iranian regime. A complete breakdown of current diplomatic negotiations, a further strengthening of economic sanctions, or the use of military force against Iranian nuclear facilities could all potentially trigger an asymmetric retaliation.

Should that happen, the United States will find itself confronted with a new, and qualitatively different, cyber threat—one for which it is still ill-prepared. For, while the past year has seen a dramatic expansion of governmental awareness of cyberspace as a domain of conflict, serious institutional

awareness of Iran's cyberwarfare potential has lagged behind the times. So has a comprehensive governmental response to it.

It is a deficiency that the United States can no longer afford to tolerate. ■

[1] Ramin Mostaghim and Emily Alpert, "Iran's Supreme Leader Calls for New Internet Oversight Council," *Los Angeles Times*, March 7, 2012, http://latimesblogs.latimes.com/world_now/2012/03/iran-internet-council-khamenei.html.
[2] *Radio Free Europe*, January 4, 2012
[3] Steve Stecklow, "Special Report: Chinese firm helps Iran spy on citizens," Reuters, March 22, 2012, http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322.
[4] See, for example, Saeid Golkar, "Liberation or Suppression Technologies? The Internet, the Green Movement and the Regime in Iran," *International Journal of Emerging Technologies and Society* 9, no. 1 (2011), 50-70, http://www.swinburne.edu.au/hosting/ijets/journal/V9N1/pdf/Article%204%20Golkar.pdf.
[5] "New Cyber Espionage Virus Found Targeting Iran," Reuters, July 17, 2012, http://www.jpost.com/International/Article.aspx?id=277803.
[6] Yaakov Katz, "Iran Embarks On $1b. Cyber-Warfare Program," *Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864http://www.jpost.com/Defense/Article.aspx?id=249864.
[7] Farvartish Rezvaniyeh, "Pulling the Strings of the Net: Iran's Cyber Army," PBS *Frontline*, February 26, 2010, http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-the-strings-of-the-net-irans-cyber-army.html; Alex Lukich, "The Iranian Cyber Army," Center for Strategic & International Studies, July 12, 2011, http://csis.org/blog/iranian-cyber-army.
[8] "STUXNET has Returned Home," *Kayhan* (Iran), July 27, 2011. (Author's collection).
[9] Author's personal communication, August 17, 2011.
[10] Brian Ross, "What Will Happen to the US if Israel Attacks Iran?" ABC News, March 5, 2012, http://abcnews.go.com/Blotter/israel-attacks-iran-gas-prices-cyberwar-terror-threat/story?id=15848522#.T4g5tqvY9Ll.
[11] Kevin Coleman, "Iranian Cyber Warfare Threat Assessment," Defense Tech, September 23, 2008, http://defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment/.
[12] James Clapper, testimony before the Senate Select Committee on Intelligence, January 31, 2012.

CYBERSECURITY: FROM EXPERIMENT TO INFRASTRUCTURE

By Abraham R. Wagner

The rapid evolution of cyberspace has clearly been one of the greatest technological revolutions in recorded history. What began as a Defense Department experiment at the Advanced Research Projects Agency (ARPA, later DARPA) in the late 1960s has transformed almost all aspects of life with new technologies as well as related applications available on a myriad of new devices. Since the transition from the ARPAnet to the Internet in 1989, there has been an explosive growth in e-mail, the web and net-based applications of a magnitude never anticipated.

Security and privacy were not essential elements of the original ARPAnet design and much of what was done in the aftermath can be characterized as "too little, too late." At the outset, the ARPAnet was an experiment to test a new concept in optimizing network resources with "switched packet" technology as an alternative to traditional "line switching." E-mail was not even a part of the concept, the web did not yet exist, there were no browsers or net-based content, and there were no early commercial or national security applications.

Apart from DARPA's developmental work, a wide range of users—including the government, commercial firms, educational institutions and others—acquired computers connected to local and later wide area networks. With the transition to the Internet, these LANs and WANs were easily given global connectivity at exceedingly low cost. For the first time in history, the marginal cost of worldwide communications fell to almost zero, as the development of the "web" and related browsers made user interface far easier, with new applications and web-based content virtually exploding.

These developments took place in what was increasingly referred to as "cyberspace" or often simply "the net," with a large number of new firms offering an enormous range of web applications and services heretofore never dreamed of. Few entrants into cyberspace were aware of or cared about the myriad of security vulnerabilities which existed at all hardware and software levels. For well over a decade, the prevailing notion was that if there were problems, it must be somebody else's job to fix them.

Early vulnerabilities and security efforts

The commercial world was quick to adopt the

Dr. Abraham R. Wagner *is Professor of International & Public Affairs at Columbia University, and Senior Research Scholar at Columbia's Arnold A. Saltzman Institute of War & Peace Studies. He served for over 30 years in various U.S. Government posts at the National Security Council, the Intelligence Community, and Department of Defense, including the Defense Advanced Research Projects Agency (DARPA) at the time of the transition to the Internet.*

net and offer a vast range of applications, but was largely unwilling and most often uninterested in paying to secure it. Even large banks failed to address the problem until they had been robbed of massive sums of money. For their part, national security users were not much better. They quickly embraced cyberspace and networked systems, as they were highly cost-effective and offered a range of important capabilities, but initially failed to address critical vulnerabilities.

From the outset of the Internet programmers recognized a number of vulnerabilities, both in computer operating systems as well as server design. Early attacks generally involved malware which disabled vulnerable computers and later exploited data which was not protected and stole larger amounts of data from commercial and government servers connected to the net. Recognizing the problems, Microsoft continued to distribute "fixes" and "patches" to deal with some vulnerabilities while third party vendors like Norton sold security software that attempted to deal with a wider range of malware, installed firewalls, and gave users regular updates as new threats were identified.

The commercial world was quick to adopt the net and offer a vast range of applications, but was largely unwilling and most often uninterested in paying to secure it.

These early entrants into the field saw the threat from malicious net activity and tried to protect users from malware, removing suspicious code such as viruses, worms and Trojans from infected computers. Other firms offered encryption software, such as PGP, enabling their users to protect sensitive files while a secure version of net protocol (:/https) enabled "secure" transactions over the web. In some ways, cyberspace was becoming safer and more secure for many users, but the adversarial threat was advancing at an even greater pace as well.

While the early threats to cyberspace came largely from hackers such as bored high school kids and disgruntled system administrators, the past decade has witnessed the evolution of far more serious cyber threats from expert criminals as well as well-trained military units assigned to cyberwarfare missions. Debate continues over the range of potential threats, ranging from annoying denial of service to the type of apocalyptic attack seen in films such as "War Games" and others. Some analysts write about a "Digital Pearl Harbor," which could involve massive denial of net services, widespread theft of data, or quite possibly the corruption of data being sent over the net.

A lagging response

It is the unfortunate reality that national policy toward cybersecurity during the 1990s, the Internet's first critical decade, was in large part either non-existent, or otherwise badly managed, poorly funded, and in some cases simply absurd. As the net literally exploded in terms of users and applications, and evolving threats were seen, there was no national consensus as to whose responsibility it was to secure cyberspace and respond to the threats. While the government and the military became large-scale users, and therefore the proverbial "pig at the trough,"

little was done by the Defense Department and the military services to protect this vital resource. As a whole, government saw this as a responsibility of the commercial net providers and third party vendors, and funded programs to deal with it were minimal and inadequate.

What the nation failed to see at that time was the reality of the cyber threat problem, mostly from overseas. As national security, government, and finance became large net users, they also became lucrative targets for both major criminal enterprises, such as those in Russia, as well as foreign military forces, such as those in China, who foresaw the potential for cyberwarfare. At best, the nation was still focused on defense against annoying hackers and lower level threats, and not looking to the rapidly evolving threat environment. DARPA's efforts, for example, were limited to funding of the Computer Emergency Response Team (CERT) at Carnegie-Mellon University, and the FBI's National Infrastructure Protection Center (NIPC) was staffed entirely by four contractor personnel—paid for by CIA—and no FBI staff at all.

On the offensive side, U.S. policy was still in a very early stage, with no serious basis in policy and actual programs limited to a few very small and poorly-funded activities within the intelligence agencies and DoD. Virtually no thought was given to how cyberwarfare efforts could be developed and integrated into larger national policies involving traditional "kinetic warfare."

While the 9/11 attacks themselves had little to do with cyberwarfare, they did provide a catalytic shock to the Intelligence Community and the military in terms of looking far more seriously at new threats. Internet use by terrorists and others now became a serious subject of interest. Intelligence programs to focus on net traffic which languished in the 1990s received new attention and badly needed funding. At the same time, a number of early cyber-attacks—such as Moonlight Maze (from Russia, 1999), Titan Rain (from China, 2004), and others—attacking DoD and other critical systems drove home the reality of the increasing cyberwarfare threat.

While an overall national policy was still lacking, at least DoD and the Intelligence Community undertook a number of organizational changes responsive to the evolving threats. Air Force and Navy cyber commands were designated, along with a unified Cyber Command (CYBERCOM), with the Director of the National Security Agency being dual-hatted as the CYBERCOM Commander. Shortly after taking office, the Obama administration appointed a White House "cyber czar" and undertook the development of a national strategy, which was announced in May 2011, but little has been done to substantively implement it.

Toward a strategy

Starting in 1999, increasing cyber attacks from foreign groups seriously raised the specter of cyberwarfare as a realistic arena for future conflict. Analysts and lawyers began a debate as to how to prosecute this new type of warfare, which has no geography and differs from the traditional model of kinetic warfare, and what "rules" of warfare, if any, would apply. A key consideration was the extent to which the essential elements of loss of life and destruction of property—the two cornerstones of the kinetic model—might apply in the cyberwar context.

Much of the current debate in this area revolves around whether specific operations can be categorized as a military operation, in which case Title 10 of the United States Code (USC) applies, or whether such activities are espionage, in which case they rightly fall under the Code's Title 50. In the case of Title 10, the international rules of war apply, while in the case of Title 50, any cyber operations come under the category of espionage where there are no international rules, and unlikely to be any in the foreseeable future. Here the domestic laws of target nations would apply, and anyone caught engaged in espionage is subject to local laws which can be truly draconian.

But people matter too. Implementing a successful national strategy for cyberspace must necessarily start with building the technology base, and in this area largely involves educating people with the skills necessary to meet the emerging challenges. It is also an area that simply requires the "best and the brightest" to create the type of software needed. It is not one where hiring those that are able to pass a polygraph, or are recruited to meet some artificial hiring quota will suffice. Cyberspace defense and offense cannot be another experiment in workfare or a labor force of the mediocre.

Implementing a successful national strategy for cyberspace must necessarily start with building the technology base, and in this area largely involves educating people with the skills necessary to meet the emerging challenges.

Educating the necessary cyberspace workforce will also require a new level of commitment to the nation's universities, possibly using the model of the Eisenhower administration in responding to the Cold War challenges of the "space race." At that critical point in history the nation undertook a series of coordinated initiatives starting with substantial government investment in science and math education, under the National Defense Education Act (NDEA) and others. At the same time, the government initiated new technology agencies, such as ARPA, the National Science Foundation (NSF), and several others.

Taking this path again in the context of cyberspace makes good sense, and it is reasonably certain that the universities are not going to meet this challenge with only their own resources. In the current economic climate, the major private universities are constrained, while most public universities are under enormous economic pressure. While there is sound logic that shows there are increasing numbers of jobs in cyberspace, the fact does not seem compelling enough to overcome the level of inertia in education today.

Money matters as well. It is increasingly clear that the government cannot continue to be "the pig at the trough" in terms of massive net use; fail to adequately fund effective security programs; and maintain the false expectation that the private sector will recognize the full scope of the problems and remedy them.

There is an old adage within the government that "no program is better than an

underfunded one." For the decade of the 1990s, the government failed to adhere to this maxim where cyberspace defense and offense were concerned. The nation has been paying the price. DARPA, the DoD agency that "invented" the net, has limited funds at best to tackle the current set of problems, and can only be expected to make the types of high-risk investments in future technologies that are its forte. NSA, another DoD agency, has finally assumed an increasing role in both defensive and offensive domains of cyberspace. Its programs are also co-located and coordinated with CYBERCOM, which is important synergy. Efforts here need continued strong support, away from any budget-cutting initiatives.

At least on the defensive side, the tasks cannot all be left to DoD and the intelligence agencies. Without exception, all other government agencies have become major users of cyberspace. Therefore, they also need to become partners in its ongoing protection.

The final piece of the puzzle is industry. Aside from inadequate funding, one reason national policy on cyberspace failed in the 1990s was a fundamental misunderstanding of the role industry could and would play in securing the net. In part, there were unreasonable expectations that the technology companies would recognize the full range of vulnerabilities and fix them—independent of government support. It was also believed that user demands, from both the public and private spheres, would drive them to do so.

This belief was only partially correct; what was done was inadequate, and not sufficient to meet the major threats evolving in foreign nations. What is needed now is a more realistic approach to industry involvement on several levels. At the outset, it is essential to recognize that industry built cyberspace and they will fix it, irrespective of who pays. By and large the government can only write checks—not computer code. Even in the most sensitive areas the actual work is out-sourced to commercial firms with few programmers being government employees. DARPA itself does no work internally, and only funds contractors for their development efforts. Here the nation needs to move to a model where the technology companies that dominate cyberspace are made a more integral part of the process.

In the final analysis, the nation needs to look ahead at what the solution is going to be, and work back from that, making sure that the technology base and the supporting industrial base can meet the very real threats and challenges ahead. ■

THE U.S. RESPONSE TO CYBERSECURITY THREATS

By Frank J. Cilluffo

In counterterrorism, there have been two major breakthroughs since 9/11 that together have significantly enhanced our overall counterterrorism posture. The first is the synchronization of Title 10 and Title 50 of the United States Code (USC), harmonizing military and intelligence functions in prosecuting the War on Terror. The second has been the increased practice of information sharing among agencies involved in the counterterrorism fight. While not a prefect analogy, these breakthroughs and "lessons learned" also have application in our efforts to defend against cyber threats.

To date, the cybersecurity community has not reached anything approaching the level of maturity now displayed by the U.S. counterterrorism community. Its current state is akin to where anti-terror efforts found themselves shortly after the attacks of 9/11.

With respect to the synchronization of Titles 10 and 50 in the cyber domain, we have still to codify rules of engagement and pursue a more proactive stance. With respect to information sharing, significant impediments continue to exist in both law and practice.

This is best demonstrated by the relationship between the public and private sectors A constructive relationship must be built between these two sectors in order to facilitate situational awareness founded on threat-related information sharing and protection efforts. The cyber threat (and supporting technology) has markedly outpaced prevention and response efforts. In short, our ability to network is far greater than our ability to protect networks. Despite multiple incidents that could have served as galvanizing events to shore up U.S. resolve to formulate and implement the changes that are needed, we as a country have yet to take those necessary steps.

Understanding the threat

The current cyber threat confronting the United States is multifaceted, and evolving. It ranges from individual hackers to hacktivists to criminal or terrorist organizations to nation-states or those that they sponsor. This complex threat spectrum affects the public and private sectors, the interface and intersections between them, as well as individual citizens. National security, economic security, and intellectual property are just some of the major interests at stake. A differentiation needs to be made among nuisance hacks, acts of espionage and true cyber attacks so that we can proportionately defend against the most egregious threats.

Frank J. Cilluffo *is director of The George Washington University Homeland Security Policy Institute. He previously served as Special Assistant to President George W. Bush for Homeland Security, and in senior policy positions at the Center for Strategic and International Studies.*

Yet today, media reporting is haphazard and everything seems to be thrown into the same basket, causing confusion and impeding attention on what really matters. In reality, hacks of websites are akin to graffiti in cyberspace, they are not the same as an exploit on our SCADA systems or a cyber equivalent of intelligence preparation of the battlefield (IPB), in order to map out our critical infrastructures. It is also important to note that while technology will continue to advance and its application in terms of tactics, techniques and procedures will continue to evolve, human behavior remains the same and is at the root of the challenge.

From a homeland security perspective, at least in terms of sophistication, foreign states are our principal concerns—in particular those that pose an advanced and persistent threat, namely Russia and China. The cyber threat is unique in that it is made for plausible deniability. Russia has developed very sophisticated capabilities, and many of its acts of cyber espionage and cyber attacks go unattributed or unreported. China, while highly sophisticated, may not meet Russia's capabilities yet, but it makes up for it in the sheer number of attacks and acts of espionage that it commits.

Other countries worthy of attention are North Korea and Iran. These two actors lack some technical capability at the moment, but make up for it in sheer intent. Additionally, in the Iranian case, the government is investing heavily in cyber capabilities and may well turn to their proxies as a force multiplier.

The cyber threat (and supporting technology) has markedly outpaced prevention and response efforts. In short, our ability to network is far greater than our ability to protect networks.

Legislative needs

To adapt, we need legislation now—while cooler heads can prevail and not wait until after a major incident. Any legislation passed after such an incident would be much more draconian than what we could pass currently.

The Cyber Intelligence Sharing and Protection Act (CISPA) passed the House in late April, and it would allow for the sharing of cyber threat information between the U.S. government and the private sector. This represents a step in the right direction. The debate in the Senate is more polarized, but some lawmakers—namely Senators Kyl and Whitehouse—have forged a compromise group among the bills currently proposed.

It is important to note in light of these ongoing debates that security and privacy are not mutually exclusive. There is a need for standards—these should be identified and self-initiated by the private sector, across critical industries and infrastructures, together with an enforcement role for government in order to protect and promote, not stifle, innovation. Owners and operators of critical infrastructure should be called upon to define and implement standards and best practices. Since owners and operators know the intricacies and vulnerabilities of their sectors better than anyone else, this self-initiated approach will ensure that standards

are customized and effective while avoiding unnecessary or duplicative regulation. A trusted third party could ensure compliance with standards and best practices by granting a "Good Housekeeping" seal of approval to critical infrastructures that meet the bar.

In addition to addressing the "sticks" within the proposed cyber legislation, we must also address the issue of the "carrots". The business case for cyber, including incentives, still needs to be built. A mix of incentives is needed, to include tax breaks, liability protections, and insurance premium discounts, for private owners and operators of critical infrastructure to take the steps needed to help improve our overall level of security. Furthermore, a mechanism must be put in place to encourage and enable information sharing between the public and private sectors.

We cannot expect the private sector to protect and defend itself, at least not against foreign government intelligence services like those of Russia, China, Iran or North Korea. Moreover, the federal government has a responsibility to share threat information (i.e., signatures, hostile plans and techniques to degrade, disrupt or destroy systems) that places our critical infrastructures at risk. The pilot program introduced within the confines of the defense industrial base offers a solid starting point, and an example of a promising information-sharing environment.

Moving forward, the United States should develop and clearly articulate a cyber-deterrence strategy to dissuade, deter and compel our cyber enemies. Underpinning any comprehensive strategic approach is the recognition that 1) we simply cannot firewall our way out of the problem, and 2) that the initiative remains with the attacker. Such a deterrence policy should apply generally, and also in a tailored manner that is actor/adversary specific. A solid general posture could serve as an 80 percent solution, neutralizing the majority of threats before they manifest fully. This, in turn, would free up resources (human, capital, technological, etc.) to focus our limited resources and bandwidth on the high-end of the threat spectrum and on those which are most sophisticated and persistent.

Moving forward, the United States should develop and clearly articulate a cyber-deterrence strategy to dissuade, deter and compel our cyber enemies.

Balancing the response

To operationalize these recommendations, we must draw lines in the sand. Preserving flexibility of U.S. response by maintaining some measure of ambiguity is useful, so long as we make parameters clear by laying down certain markers or selected redlines whose breach will not be tolerated. Cybersecurity by definition is transnational in nature and will require some level of transnational solutions, yet it must not be approached like an arms control treaty (i.e., attribution and verification are still a ways away).

More investment needs to be made in our offensive capability as well—according to open source reporting, we currently we spend 90% on defense and 10% on offense.

If multiple stakeholders could agree on such an approach, we as a country would be able to begin to address our risk before we are forced to do so by events. ■

Ilan Berman *Chief Editor*

Rich Harrison *Managing Editor, Graphic Design and Layout*

MANUSCRIPTS SHOULD BE SENT TO the attention of the Editor at 509 C Street, NE, Washington, DC 20002, or submitted via email to defensedossier@afpc.org. The Editors will consider all manuscripts received, but will assume no responsibility regarding them and will return only materials accompanied by appropriate postage. Facsimile submissions will not be accepted.

EDITOR'S NOTE: The opinions expressed in the *Defense Dossier* (ISSN 2165-1841) are those of the author(s) alone and do not necessarily represent the opinions of the American Foreign Policy Council.

About the American Foreign Policy Council

For nearly three decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies. AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.

DEFENSE DOSSIER

American Foreign Policy Council

American Foreign Policy Council
509 C Street, NE
Washington, DC, 20002
www.afpc.org