2016

SPRING
VOLUME 2

STRATEGIC PRIMER: CYBERSECURITY

Current capabilities and emerging threats

CYBER THREATS & NATIONAL SECURITY

The American Foreign Policy Council (AFPC) is dedicated to advancing the prosperity and security of the United States. AFPC's Defense Technology Program launched the Strategic Primer initiative to educate Congressional staffers (and the general public) on technologies that affect U.S. national security. The Primers depict balanced representations of the potential benefits and limitations of a particular technology, its history and uses, and potential threats posed by adversarial use of the technology.

This work seeks to provide insights into current and future cybersecurity threats, and public policy responses to them. It provides a succinct and informative background of the cyber capabilities of the United States, as well as that of our adversaries, discusses the various challenges that are posed today by cyber threats, and offers policy recommendations about how best to mitigate them.

TABLE OF CONTENTS

PROJECT TEAM

Director:	Rich Harrison
Editor:	Ilan Berman
Graphic Design:	Ozzie Chung
Primary Researchers:	Peter Leenen
	Hadley Nagel
	Emily Zavrel
Research & Content:	Simone Worthy
	Paige Rotunda
	Nishant Atal

WHAT IS A CYBER ATTACK?

In 2013, experts commissioned by the NATO Cooperative Cyber Defense Center of Excellence released the Tallinn Manual, which outlines international law principles of both the *jus ad bellum* (recourse to the use of force) and the *jus in bello* (conduct of war) in cyberspace. In this manual, a cyber armed attack, as it relates to international law, is any "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[1] This definition differentiates cyber attacks from cyber espionage, which is identified as "any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party."[2]

WHAT IS CYBERSECURITY?

The National Initiative for Cyberspace Careers and Studies (NICCS), an organization within the Department of Homeland Security (DHS), defines cybersecurity as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."[3]

ADDRESSING THE THREAT

This primer focuses on threats posed by nation states attempting to negatively affect U.S. national security through cyber intrusions and attacks. However, non-state actors also play an increasingly large role in the cyber threat matrix. Though not addressed directly here, such sub-state actors are utilized by countries and also pose a substantial threat to the U.S. economy.

CYBERSECURITY: AN OVERVIEW

President Obama has affirmed that the "cyber threat is one of the most serious economic and national security challenges we face as a nation," and that "America's economic prosperity in the 21st century will depend on cybersecurity."[4] Cyber operations have already detrimentally affected both the economy and the national security of the United States, and will continue to do so. America, therefore, must protect itself from cyber attacks emanating from nations such as China, Iran, North Korea, and Russia.

CYBER OPERATIONS

Cyber threats are enabled by a set of technical circumstances that are prevalent today. These include: pervasive use of insecure software languages by computer programmers, a bias toward trust in the design of computing hardware and internet protocols, and the increasing interconnectedness of critical systems. Cybersecurity operations typically come in four types: 1) disclosure - when secret information is leaked; 2) theft (also called fraud) - when something of value is stolen; 3) integrity - when something of value is intentionally corrupted; and 4) denial of service - when some service is intentionally blocked.[5] Although far less common, a cyber attack also may be utilized to achieve physical destruction of a target.

VULNERABILITIES

These different operations can have devastating effects without an opponent ever having to leave their home country. Cyber operations could be (and some have been) initiated against: financial systems, satellites in orbit, nuclear and conventional power plants, transportation systems, telecommunications services, emergency services, government infrastructure, and utilities such as water supplies.[6] It has been observed that "[b]ecause of the interlocking nature of major global financial institutions, including individual banks, even a cyber attack on one nation's financial infrastructure could have a fast-moving ripple effect, undermining confidence globally… cyber attacks on banks could unravel the entire global financial system."[7]

MANAGING RISK

If an attack took place on an electric power grid, the results could be catastrophic: "Having an attack take place in many locations simultaneously, and then happen again when the grid comes back up, could cripple the economy by halting the distribution of food and other consumer goods, shutting down factories, and forcing the closure of financial markets."[8] This isn't to say that such an attack would be easy, or even that it is likely. Rather, it underlines the vulnerability of computing systems to manipulation and disruption by attackers. Industrial control systems (ICS), with their long lifespans and requirements for frequent updates and security fixes, are particularly vulnerable to attack (legacy ICS are seldom updated). As adversaries discover these vulnerabilities, it is imperative that the U.S. is proactive and prepared to react both defensively and offensively.

COMMON CYBER TERMS

Common cyber terms as defined by the Department of Homeland Security cybersecurity division.[9]
**Terms with an asterisk are defined by Strategic Primer authors.*

air gap - To physically separate or isolate a system from other systems or networks.

attack - An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

bot - A computer connected to the Internet that has been surreptitiously / secretly compromised with malicious logic to perform activities under remote command and control of a remote administrator.

botnet - A collection of computers compromised by malicious code and controlled across a network.

bug - An unexpected and relatively small defect, fault, flaw, or imperfection in an information system or device.

cloud* - A network of servers connected to the internet which host data, run applications, and process information remotely.

cyberspace - The interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

data breach - The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

denial of service - An attack that prevents or impairs the authorized use of information system resources or services.

distributed denial of service (DDoS) - A denial of service technique that uses numerous systems to perform the attack simultaneously.

firewall - A capability to limit network traffic between networks and/or information systems. A hardware/software device or a software program that limits network traffic according to a set of rules of what access is and is not allowed or authorized.

hacker - An unauthorized user who attempts to or gains access to an information system.

information sharing - An exchange of data, information, and/or knowledge to manage risks or respond to incidents.

insider threat – Any "current or former employee, contractor, and even business partner who has or had access to an organization's system, network, or data. The insider has intentionally exceeded or used that access in a manner that typically negatively affected the confidentiality, integrity, or the availability of the organization's information or information system."[10]

malware - Software that compromises the operation of a system by performing an unauthorized function or process.

phishing - A digital form of social engineering (conning) designed to deceive individuals into providing sensitive information.

spyware - Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

trojan horse - A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

virus - A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

vulnerability - A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

zero-day (0-day)* - A vulnerability in software that is unknown to the software vendor and is open to exploitation.

HISTORY OF CYBER OPERATIONS

70,000 cybersecurity incidents occurred on Federal agency networks in FY 2014. Over the past ten years, cyber operations have become more frequent and complex. The following timeline highlights a few of the more notable operations during this time.[11]

2003

Titan Rain (PRC) Chinese hackers gain access to U.S. federal agency and defense contractor computer networks and government agencies in order to steal sensitive information.[12]

2004

(DPRK) Hackers gain access to 38 out of 88 South Korean military wireless communication networks.[13]

2006

(Russia) Russia used cyber operations as a force multiplier during the kinetic war with Georgia. Hackers used DDoS attacks on government websites and communication platforms.[16]

(DPRK) The U.S. State Department's network is breached by hackers looking for sensitive information.[14]

2007

(Russia) Russian hackers target Estonian government, bank, and media websites during heightened tensions between Russia and Estonia.[15]

(PRC) Targeted malware attack against U.S. defense contractors compromised the $300 billion Department of Defense Joint Strike Fighter project.[17]

2008

Duqu (U.S.) Similar to Stuxnet (though not capable of destruction), Duqu is deployed to search for information that could be used in future attacks in order to disrupt industrial control systems.[19]

2009

Gauss (U.S.) Described as a "nation-state sponsored cyber-espionage toolkit," the malware is identified as having primarily stolen passwords and banking credentials.[20]

Flame (U.S.) Sophisticated cyber espionage platforms with the capability of recording audio, taking screenshots, logging keystrokes, and capturing network traffic. It can infect machines shared on the same local network and, once finished, could wipe itself from the machine, leaving no trace.[21]

2010

Stuxnet (U.S./Israel) Malware designed to physically destroy programmable logic controllers targets centrifuges in air-gapped Iranian nuclear facilities.[18]

2011

Shamoon (Iran) Cyber attack on Saudi Arabia's national oil and gas company, Saudi Aramco, that erased data from 30,000 computers.[22]

(Iran) Similar malware to Shamoon, the internal network of RasGas, a Qatari natural gas company, was shut down for several days.[23]

2012

(China) Members of China's People's Liberation Army breach databases from the Office of Personnel Management, stealing records belonging to roughly 22 million federal employees and contractors. [26]

2014

(DPRK) State-sponsored hackers breach media conglomerate Sony's networks, stealing close to 100 terabytes of data over the course of a year before wiping data off their servers.[25]

2015

(Iran) First instance of a nation state attack on a U.S. business (Sands Casino) with the sole purpose of shutting down operations in response to the CEO's political views.[24]

CHINA

2016 WORLD THREAT ASSESSMENT

"China continues to have success in cyber espionage against the US Government, our allies, and U.S. companies. Beijing also selectively uses cyberattacks against targets it believes threaten Chinese domestic stability or regime legitimacy."[27]

BACKGROUND/CYBER DOCTRINE

China's interest in cybersecurity dates back to 1995, when the *Liberation Army Daily*, a media outlet for the People's Liberation Army (PLA), identified two critical areas of information war: information protection and information attack.[28] By 1999, the PLA had placed information warfare on equal footing with the four traditional war domains (land, sea, air, space) and created a dedicated military branch for the discipline.[29] Chinese military writings clearly view cyber warfare as a means to "force an adversary to capitulate before the onset of conflict."[30] China's leaders have actively encouraged the country to become a leading cyber power. In 2012, then-General Secretary Hu Jintao stated "We should attach great importance to maritime, space and cyberspace security. We should make active planning for the use of military forces in peacetime, expand and intensify military preparedness, and enhance the capability to accomplish a wide range of military tasks, the most important of which is to win local war in an information age."[31] More recently, in 2015, the Chinese Ministry of Defense released a military strategy declaring that, "[a]s cyberspace weighs more in military security, China will expedite the development of a cyber force, and enhance its capabilities of cyberspace situation awareness, cyber defense, support for the country's endeavors in cyberspace and participation in international cyber cooperation, so as to stem major cyber crises, ensure national network and information security, and maintain national security and social stability."[32]

CYBER OPERATIONS PERSONNEL

The organization of China's cyber forces dates back some years. In 1997, "a 100-member elite corps was set up by the Central Military Commission to devise 'ways of planting disabling computer viruses into American and other Western command and control defense systems."[33] More recently, "the People's Liberation Army (PLA) announced on 20 July 2010 that it had established an 'Information Protection Base' under the General Staff Department."[34] In May of 2011, a Ministry of Defense Spokesman announced a cyber "Blue Army" had been assembled to provide cybersecurity for the nation (operating budget of $1.54 million).[35] Chinese funding for cyber operations has dramatically increased over time. As of 2015, reports claim that the country's cyber budgets tally in the hundreds of millions to billions, and increase annually at estimated rates ranging from 20-33 percent.[36] The main known cyber divisions are the Ministry of State Security (intelligence collection and counter-intelligence/espionage), Ministry of Public Security (protection of critical infrastructure), and the PLA General Staff Department, 3rd Department (signals and intelligence collection, similar to U.S. NSA).[37] **Unit 61398** is an elite hacking unit of the PLA (3rd Dept., 2nd Bureau) based in Pudong, Shanghai.[38] The unit coordinates directly with the Communist Party of China and has access to state-run companies for extra resources. It specializes in the theft of intellectual property relating to both strategic and emerging industries as listed by China's Five Year Plan.

In many instances, Chinese cyber forces utilize decentralized operations. With nearly 700 million online users in China, the PRC has the ability to recruit from a veritable army of private citizens both willing and able to advance its goals, making the challenge of attribution even harder. In fact, there have been several cases of cyber activity in which collaboration between hackers and Chinese civilians has been apparent.[39]

CYBER TARGETS

China targets several countries, but their principal focus is on the U.S. government and its defense contractors. The PRC uses cyber espionage activities to bolster its research and development and enhance its military modernization in addition to providing Chinese corporations with an economic advantage.[40] In a conflict, China will likely target U.S. military systems in order to delay and disrupt the deployment of American forces.[41] The PLA also aims to disrupt U.S. operational and tactical communications, its computer networks operations, and its navigational and targeting radars, all of which is detrimental to U.S. military operations.[42]

Many U.S. government agencies and critical infrastructure nodes have fallen victim to Chinese cyber attacks. Although the Chinese deny any involvement, in 2009 Chinese cyber spies were accused of collaborating with Russia in the hacking of the U.S. electrical grid, leaving behind programs that have potential to be disruptive and even destroy parts of the system.[43] China has been using cyber attacks against private sector contractors, particularly those that handle classified information, as a means of extracting valuable information from the U.S. government. For example, in the span of a year, "the Chinese government successfully penetrated U.S. Transportation Command contractors about twenty times." These activities can assist the Chinese government in hindering programs and networks that support the U.S. national defense.[44]

IRAN

2016 WORLD THREAT ASSESSMENT

"Iran used cyber espionage, propaganda, and attacks in 2015 to support its security priorities, influence events, and counter threats—including against U.S. allies in the region."[45]

BACKGROUND/ CYBER DOCTRINE

Iran divides its cyber strategy into offensive and defensive segments. Offensively, Iran's cyberspace strategy is part of its asymmetric warfare doctrine. Similar to guerilla warfare or terrorism, offensive cyber capability is viewed as a tool to significantly damage a superior adversary. Defensively, Iran's goals are to both protect critical infrastructure from cyber attacks and ensure opponents of the regime do not utilize cyberspace for communication and information exchange. Iran has sought to bolster its mission in cyberspace by reaching out to allies and other actors. In 2012, Iran inked a technology treaty with North Korea, stipulating that the two nations would collaborate on research, IT information sharing initiatives, and jointly work to counter "common enemies" in cyberspace.[46] In addition to collaborating with the DPRK, Iran has attempted to hasten the pace of its cyber program by eliciting expertise from Russian cybersecurity experts and cyber criminal groups.[47] Iran's cyber expertise is purposely dispersed in order to create an "effective system of proxies," including the Syrian Electronic Army (SEA).[48] There are also proxy hacker groups loosely tied to the Iranian government which carry out attacks, including the al-Qassam Cyber fighters and Cutting Sword of Justice, an Iranian hacker group tied to the government.

CYBER OPERATIONS PERSONNEL

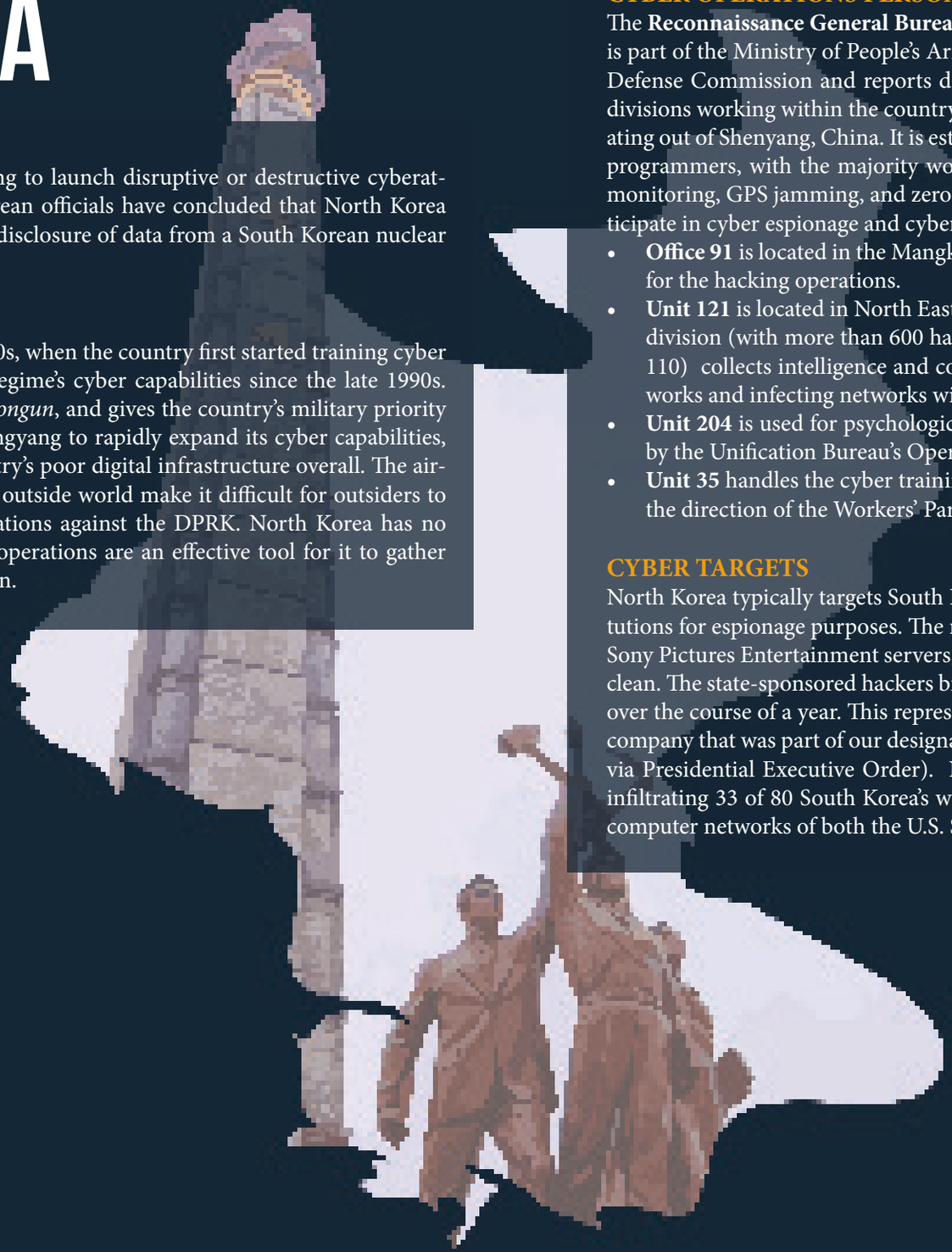
The Stuxnet attack on Iranian nuclear facilities served as a wake up call to Tehran, and prompted the Iranian government to invest heavily in cyber capabilities. In 2011 alone, the regime is known to have allocated $1 billion to erect a national cyber program aimed at improving cyber defense and technology.[49] Significant funding has continued since, and President Hassan Rouhani recently increased the cybersecurity budget by a factor of 12.[50] Iran previously could have been classified as a second tier cyber actor, in terms of offensive capabilities. Over time, however, it has increased both the scope and the sophistication of its cyber effort, and is now on footing closer to that of China and Russia.[51]

- **High Council of Cyberspace** (*Shoray-e Aali-e Fazaye Majazi*) - Established in 2012 by Supreme Leader Ali Khamenei to serve as the governing body for all cyber initiatives. It consists of "the highest-level Iranian authorities such as the president, the heads of the judicial power and the parliament, the head of the state-run radio-television, the commander-in-chiefs of the IRGC and the police, the ministers of Intelligence, Telecommunication, Culture, Science, etc."[52] In addition, the Iranian Revolutionary Guard Corps oversees a significant portion of cyber operations.[53]
- **Cyber Defense Command** (*Gharargah-e Defa-e Saiberi*) - Established in November 2010, this organization is charged with protection of national critical infrastructure from cyber threats and is a overseen by the Passive Civil Defense Organization (*Sazeman-e Padafand-e Gheyr-e Amel*), a subdivision of the Joint Staff of the Armed Forces (*Setad-e Kol-e Niruhay-e Mosalah*)."[54]
- The **Iran Cyber Army** is the group of cyber experts who conduct offensive cyber and intelligence gathering operations, but is not officially connected to any government agency, but is more than likely affiliated or directed by the IRGC.[55]

CYBER TARGETS

In the past, Iran's most invasive cyber operations have primarily targeted the United States and Saudi Arabia, but their reach has been evident across the globe. In 2014, a report by cybersecurity firm Cylance, entitled *Operation Cleaver*, outlined Iran's extensive activities in cyberspace, including its targeting of U.S. critical infrastructure, such as the penetration of chemical and energy companies, defense contractors, universities, and transportation providers.[56] According to the report, there was, "no direct evidence of a successful compromise of specific Industrial Control Systems (ICS) or Supervisory Control and Data Acquisition (SCADA) networks." However, Iranian cyber operatives were able to exfiltrate extremely sensitive data from many critical infrastructure companies, allowing them to directly affect the systems they run. This data could enable them, or affiliated organizations within the Iranian bureaucracy, to target and potentially sabotage ICS and SCADA environments with ease."[57] Cutting Sword of Justice claimed responsibility for creating the Shamoon virus, which targeted Aramco along with other Saudi petroleum companies, destroying tens of thousands of computers.[58] Additionally, in 2015 Iranian hackers claimed responsibility for compromising the back office system for a New York dam, further demonstrating the need to protect critical infrastructure from cyber attack.[59]

NORTH KOREA



2016 WORLD THREAT ASSESSMENT

"North Korea probably remains capable and willing to launch disruptive or destructive cyberattacks to support its political objectives. South Korean officials have concluded that North Korea was probably responsible for the compromise and disclosure of data from a South Korean nuclear plant."[60]

BACKGROUND/ CYBER DOCTRINE[61]

North Korea's cyber program dates back to the 1980s, when the country first started training cyber specialists. The Pentagon has been aware of the regime's cyber capabilities since the late 1990s. North Korea's first military doctrine is known as *Songun*, and gives the country's military priority over resources and strategy. This has allowed Pyongyang to rapidly expand its cyber capabilities, which are under military control, despite the country's poor digital infrastructure overall. The air-gapped networks and minimal connectivity to the outside world make it difficult for outsiders to conduct reconnaissance and offensive cyber operations against the DPRK. North Korea has no clearly defined cyber warfare doctrine, but cyber operations are an effective tool for it to gather intelligence and conduct asymmetric military action.

CYBER OPERATIONS PERSONNEL[62]

The **Reconnaissance General Bureau (RGB)**, created in 2009, is North Korea's cyber command. It is part of the Ministry of People's Armed Forces, which falls under the jurisdiction of the National Defense Commission and reports directly to leader Kim Jong-un. The RGB has two main cyber divisions working within the country's borders (Office 91 and Unit 121), along with one post operating out of Shenyang, China. It is estimated that North Korea's cyber program enlists close to 6,000 programmers, with the majority working in Unit 121. Cyber capabilities include DDoS, satellite monitoring, GPS jamming, and zero-day exploits. North Korea has three additional units that participate in cyber espionage and cyber warfare (Units 110, 204, and 35).

- **Office 91** is located in the Mangkyungdae district of Pyongyang and serves as the headquarters for the hacking operations.
- **Unit 121** is located in North Eastern China at the Chilbosan Hotel in Shenyang. It is the largest division (with more than 600 hackers) and most sophisticated unit. Unit 121 (along with Unit 110) collects intelligence and conducts offensive cyber operations penetrating adversary networks and infecting networks with malware.
- **Unit 204** is used for psychological cyber operations and performing research and is governed by the Unification Bureau's Operations Department.
- **Unit 35** handles the cyber training and education of the cyber workforce. This unit falls under the direction of the Workers' Party Central Party Investigative Group.

CYBER TARGETS

North Korea typically targets South Korean and American government servers and financial institutions for espionage purposes. The regime's most infamous cyber attack is the 2014 intrusion into Sony Pictures Entertainment servers, where it not only stole information but also wiped the servers clean. The state-sponsored hackers breached Sony's networks, stealing close to 100 terabytes of data over the course of a year. This represented the first instance of a cyber attack directly against a U.S. company that was part of our designated critical infrastructure, and it resulted in sanctions (leveled via Presidential Executive Order). North Korea likewise has demonstrated its cyber prowess by infiltrating 33 of 80 South Korea's wireless military networks.[64] More recently, it has attacked the computer networks of both the U.S. State Department and Department of Defense.

RUSSIA

2016 WORLD THREAT ASSESSMENT

"Russia is assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny. Russian cyber operations are likely to target U.S. interests to support several strategic objectives: intelligence gathering to support Russian decisionmaking in the Ukraine and Syrian crises, influence operations to support military and political objectives, and continuing preparation of the cyber environment for future contingencies."[65]

BACKGROUND/ CYBER DOCTRINE[66]

Russian cyber doctrine is based on its military doctrine, which acknowledges the necessity of preventing actions aimed at destabilizing the nation, disrupting government bodies and infrastructure. The *Information Security Doctrine* approved by the Kremlin in 2000 acknowledges the importance of countering aggressive information warfare, and lists a number of methods to achieve this goal, including strategic deception and psychological operations. The four main goals of the Russian Armed Forces are 1) the use of information space in order to strengthen state defenses, 2) containment and prevention of military conflict, 3) the development of military cooperation, and 4) the formation of an international information security system in the global interest.

CYBER OPERATIONS PERSONNEL

Russia has one of the most capable cyber forces in the world, albeit one largely unknown in the public domain. There is, quite simply, very little available information regarding the hierarchy of Russia's cyber personnel. Some public action, however, is still visible. For example, the Russian Ministry of Defense is known to be in the process of forming a Cyber Command that "will be responsible for conducting offensive cyber activities, including propaganda operations and inserting malware into enemy command and control systems."[67] Cyber operation divisions are believed to be affiliated with the Federal Security Bureau (FSB).[68] There are also multiple criminal gangs that have connections to, but are not officially affiliated with, the Russian government, such as one formerly known as the Russian Business Network. Strategically, Russia exploits criminal groups unaffiliated with the government for two reasons: (1) there is no cost because criminal hacking groups are generating revenue; and (2) forensic analysis of the criminal group's computers will show no link to the Russian government, allowing plausible deniability after an attack.[69]

CYBER TARGETS

Sophisticated cyber operations have consistently targeted nation states and private sector organizations. In the past, Russian cyber operations have targeted former Soviet Republics with which the Russian government has conflicts. Eastern European patriotic hackers are using cyber operations as a supplemental means to achieve Russia's geopolitical goals. Russia implemented cyber operations before conducting traditional warfare during the 2008 Russo-Georgian war. DDoS attacks were used to disrupt Georgian information infrastructure, and an attack also targeted the control system of an energy pipeline, causing it to explode.[70] More recently, as part of its ongoing conflict with Ukraine, Russia has used cyber operations to increase pressure on the government in Kyiv, including by disabling part of the country's electrical grid. Russia also has targeted the U.S. government on numerous occasions. In July 2015, a Russian-origin cyberattack on the Pentagon succeeded in shutting down the Defense Department's unclassified email system for weeks.[71] Also in 2015, Russian hackers gained access to sensitive White House information via a phishing attack.[72]

UNITED STATES

BACKGROUND/CYBER DOCTRINE[73]

The Federal government has several agencies responsible to coordinate and execute both offensive and defensive cyber operations for the United States.

Department of Homeland Security (DHS) is responsible for the security of federal networks, promoting information sharing, and protection of U.S. critical infrastructure through preparedness and response measures.It does so by:

- Partnering with owners and operators of critical infrastructure (such as financial systems, chemical plants, and water and electric utilities).
- Housing the National Cybersecurity and Communications Integration Center (NCCIC), the "nerve center" of the government's civilian cyber and information-sharing operations.

Federal Bureau of Investigation (FBI) is responsible for response to, and investigation of, cyber incidents.

The Department of Defense (DoD) is responsible for offensive cyber operations and defense of DoD information networks (DoDIN), protection of DoD data, and assurance of DoD missions; as well as defense of the U.S. homeland and vital interests from disruptive or destructive cyberattacks of significant consequence.

- **National Security Agency (NSA)** is charged with guaranteeing "Information Assurance" which denies enemies access to classified national security information and penetration of adversary systems for espionage and disruption.
- **U.S. Cyber Command (USCYBERCOM)** centralizes and coordinates offensive and defensive cyber operations and is collocated with NSA at Fort Meade.

National Institute of Standards and Technology (NIST) is responsible for improving the cybersecurity of critical infrastructure under Executive Order (EO) 13636. It established the voluntary NIST Framework to help critical infrastructure owners and operators reduce cyber risks.[74]

Department of Defense Cyber Strategy

The official U.S. 2015 DoD Strategy has defined three primary missions: (1) To defend DoD networks, systems, and information; (2) To defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence; and (3) To provide cyber support to military operational and contingency plans.[75]

CYBER OPERATIONS PERSONNEL

Prior to 2009, the formal structure of U.S. cyber staffing was disjointed. In 2009, then-Secretary of Defense Robert Gates established a unified Cyber Command (USCYBERCOM) in the military bureaucracy under the auspices of U.S. Strategic Command. By 2016, USCYBERCOM is expected to field 133 mission teams consisting of over 6,000 personnel to defend national infrastructure, protect DoD networks, and support combatant command operations. Service element cyber divisions include 24th Air Force, 10th Fleet Cyber Command (Navy), 2nd Army/Army Cyber Command, and Marine Forces Cyber. USCYBERCOM utilizes them to conduct cyber operations as a weapon of war. It also cooperates with the CIA, DHS, FBI, and particularly with the NSA for their intelligence collecting abilities and processing.

> **Mission Statement:** "USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./Allied freedom of action in cyberspace and deny the same to our adversaries."[76]

Cyber Mission Force: 133 teams by 2018[77]

- **13 - National Mission Teams:** Defend the United States and its interests against cyberattacks of significant consequence.
- **68 - Cyber Protection Teams:** Defend priority DoD networks and systems against priority threats.
- **27 - Combat Mission Teams:** Provide support to Combatant Commands by generating integrated cyberspace effects in support of operational plans and contingency operations.
- **25 - Support Teams:** Provide analytic and planning support to the National Mission and Combat Mission teams.

Although not part of USCYBERCOM, NSA information gathering plays a lead role in offensive and defensive cyber operations. Most cyber divisions are in the classified domain, however, some information has been released about the elite NSA Tailored Access Operations (TAO). Reportedly, "TAO is responsible for developing programs that could destroy or damage foreign computers and networks via cyberattacks if commanded to do so by the president."[78] TAO is believed to be active at all hours of the day and staffed with approximately 600 members located in the Remote Operations Center (ROC).[79]

CYBER TARGETS

The United States has been involved in a number of cyber operations targeting its adversaries abroad. The most significant of these operations has likely been Stuxnet, a sophisticated package of malicious software suspected to be jointly developed by the United States and Israel and aimed at targeting Iranian nuclear facilities.[80] Although it infected computers all around the world, Stuxnet was designed to only cause disruptions when it encountered Siemens PLC control systems used to automate certain nuclear fuel processing facilities. The United States also reportedly developed Flame, a computer virus which was designed to steal information from Iranian computer networks in preparation for attempts to slow Iran's ability to develop a nuclear weapon.[81]

U.S. CYBER VULNERABILITIES

Growing dependence on cyberspace for commerce, communication, governance, and military operations has left society vulnerable to a multitude of security threats online. According to the Government Accountability Office, "Federal agencies have significant weaknesses in information security controls that continue to threaten the confidentiality, integrity, and availability of critical information and information systems used to support their operations, assets, and personnel."[82]

Critical Infrastructure is defined by DHS as: "sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[83]

> **The 16 sectors designated as critical infrastructure include:** Chemical; Communications; Dams; Emergency Services; Financial Services; Government Facilities; Information Technology; Transportation Systems; Commercial Facilities; Critical Manufacturing; Defense Industrial Base; Energy; Food and Agriculture; Healthcare and Public Health; Nuclear; and Water Systems.

The majority of cyber and Internet infrastructure is owned and operated by the private sector, including critical infrastructure and unclassified military networks. This state of affairs complicates the ability of the United States government to provide protection and ensure security. There is a large information gap between the public and private sectors, which often work under different cybersecurity standards, hindering the sharing of important information about cyber threats and the establishment of best practices for critical infrastructure companies most vulnerable to cyber attacks.[84] Within critical infrastructure, intrusions into the *Defense Industrial Base* have a particularly relevant impact on future wars. Infiltrating private defense contractor networks allows enemies to gain access to classified current and future weapon systems designs and performance specifications.

Space Systems, particularly Global Positioning System (GPS) satellites, are heavily relied upon by the U.S. military, both for determining position of forces and equipment and to deliver munitions on target. Since 2009, U.S. Central Command has relied on commercial satellites for 96 percent of its requirements.[85] This high dependency underscores the need to protect vulnerable space assets and their Internet-connected systems from cyber penetration.

Physical Dimension - In addition to digital dangers, attacks in the physical domain on cyber hardware can be equally concerning. Cutting undersea fiber optic cables or damaging the hardware at Internet exchange points (IXPs) can detrimentally impact several critical infrastructure sectors. Protecting the supply chain is another necessity. Aside from software vulnerabilities, purchasing products from non-U.S. vendors can be potentially dangerous. In 2010, the U.S. Navy purchased 59,000 counterfeited microchips from China for use in missiles and other systems; the fake chips were found to have contained backdoors allowing for remote shut off.[86]

EXECUTIVE INITIATIVES & CYBER LEGISLATION

EXECUTIVE INITIATIVES

As part of official attempts to strengthen cybersecurity, President Obama has laid out a formal *Cybersecurity National Action Plan*. This new strategy encompasses the creation of a Commission on Enhancing National Cybersecurity, the transformation of how the Government manages cybersecurity through a $3.1 billion proposal for an Information Technology Modernization Fund, and the establishment of the new position of Federal Chief Information Security Officer within the Federal bureaucracy.[87] The Administration plans to invest over $19 billion in cybersecurity in the 2017 Fiscal Year Budget (representing a 35% increase over current spending). In addition, the White House is stepping up efforts to gain more cyber professionals in the government by offering new scholarships and forgiving student loans.[88] However, it is important to note that these initiatives are a proposal, and have yet to become law.

In addition to these measures, there has been open discussion within the government about setting standards for how and when the United States is to respond to cyber attacks.[89] The need for public, specific, and uniform rules of engagement is vital to strengthening the U.S. Cyber Command. The government is also planning to better connect its defensive and offensive tasks concerning its cyber operations.[90]

CYBER LEGISLATION

- **The *Cybersecurity Information Sharing Act of 2015***[91] allows the Federal government to share cyber threat indicators and defensive measures with companies in order to enhance security of networks against cyberattacks. This law focuses on the ability to share information in real time in order to make it more useful (the private sector also shares information with the government). The law adds protection for individuals whose private information is inadvertently shared, and immunity for companies who share data with the government.
- **The *National Cybersecurity Protection Act of 2014***[92] updated the *Homeland Security Act of 2002* to restructure the National Cybersecurity and Communication Integration Center. The Center provides a platform for government agencies and private companies to share information relating to cybersecurity and incident response. While the Center is required to have representatives from federal agencies, state and local governments, and private companies, it is left to the discretion of the Undersecretary of Homeland Security on whom to include in the Center`s operations.
- **The *Cybersecurity Workforce Assessment Act***[93] directs the Secretary of Homeland Security to assess the cybersecurity workforce of the Department of Homeland Security annually for three years. In addition, it requires DHS to maintain and update both a 5-year implementation plan and a 10-year projection of the cybersecurity workforce needs of DHS.

CHALLENGES

CYBERSECURITY

The advent of the Internet has been transformative for civil society and the military. However, security was not properly integrated from the onset. As a result, ubiquitous network-connected systems and devices are left susceptible. Foreign actors can use these vulnerabilities to gain unauthorized access to sensitive systems and potentially even cause physical destruction.

There are no easily enforceable international norms and no clear rules of engagement for cyber attacks. With no proper definition for an act of war, should the international law for armed attack apply to cyber? What is considered a proportional response against a nation state or non-state actor? What is the distinction between espionage and an attack? The non-binding Tallinn Manual put forth a framework, but it is one that is not as yet universally accepted. The U.S. government (USG) is struggling to determine what role to play in this evolving discussion, while remaining prepared to fight and win any cyber conflict.

BALANCING EQUITIES

The USG successfully compromises adversary systems by finding or purchasing zero-day vulnerabilities and exploiting them. However, intentionally failing to notify software vendors of security flaws in commonly-used software places private citizens and USG agencies at risk.

In a post-Snowden era, the USG request to integrate access capabilities into U.S. tech company servers and/or attempts to circumvent their encryption protections worry citizens and could provide for potential unauthorized access by enemies.

As legislation calls for increased information sharing between companies (holding private citizen) data and the government, the USG will need to communicate with individuals that under U.S. law information shared with third party (banks, IT firms) is not private.

The USG will also need to determine when and if it is appropriate for private companies, particularly defense contractors, to initiate active defense/"hacking back" when attacked.

DHS VS. DoD JURISDICTION

Today, jurisdiction over cyber threats is divided in the U.S. bureaucracy. On the one hand, the DoD is responsible for responding to military threats emanating from hostile states. On the other, DHS is responsible for domestic security threats. Between them is a grey area known as "the seam," in which the nature of the threat is neither clearly national security nor law enforcement in nature. Cyber attacks fall in this category, and their complexity has challenged the Federal bureaucracy. The DoD is responsible for cyber attacks originating abroad and for protecting DoD networks, while DHS is responsible for coordinating protection of domestic civilian infrastructure. However, many cyber attacks originate from abroad and have the potential to disrupt critical infrastructure. Responding to cyber attacks is a difficult task for DHS because it operates without the requisite authority that would allow it to dismantle a foreign actor's network operations. In addition to these legal complications, DHS lacks the same degree of cyber operations competency as the DoD.

CYBER WEAPONS

In the future, the use of cyber weapons as an asymmetric strategy during peacetime may occur with more regularity, as will offensive cyber operations paired with kinetic attacks during actual conflict.

In the absence of international norms or clear redlines, nations can be expected to push the limits of espionage and attacks in cyberspace. The U.S. may have inadvertently opened a Pandora's Box by carrying out a cyber first strike on Iran's nuclear facilities via the Stuxnet virus. While Stuxnet was effective in causing physical damage to Iranian reactors, it had unintended consequences, because the code has been reverse engineered used by other nations in their own cyber weapons.

A major challenge in cyberspace is identifying the forces behind a cyber intrusion. Unlike conventional weapons, perpetrators can conceal their identity from their enemies. If a nation-state can not effectively attribute cyberattacks, it will be less likely to be able to deter other nations from conducting future attacks.

RECOMMENDATIONS

Full protection of the government and civil sector networks from cyber penetrations is not achievable. Damage mitigation and consequence management are the only realistic strategies, and there are areas where the U.S. can improve its cyber readiness.

Defining and Developing Deterrence

- The Director of National Intelligence has testified that the lack of an effective cyber deterrence strategy has enabled and motivated adversaries to continue committing cyber attacks.[94]
- The White House cyber deterrence policy, released as mandated by the 2014 *National Defense Authorization Act* (NDAA), lacks specificity and does not clearly articulate the consequences of conducting cyber operations.[95]

Cyber Education and Training*

- Develop methods to recruit and competitively pay the best possible cyber workforce.
- The non-IT workforce of the USG must be properly trained in "best practices" in cyberspace. This can range from understanding safe Internet use habits to being able to spot a phishing email.

Enforce Timely Software Patching*

- Major USG data breaches have occurred due to negligence and lack of timely software updates. Strategies to install updates and patch vulnerabilities to mitigate threats must be developed.

New Technologies

- Place emphasis on the development of more autonomous systems to better detect and isolate cyber threats and respond in real time.

**These recommendations are currently mandated under the Federal Information Security Management Act (FISMA), but not properly enforced.*

REFERENCES

1. Michael Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (London: Cambridge University Press, 2013), https://ccdcoe.org/tallinn-manual.html.
2. Ibid.
3. "What is Cybersecurity?" National Initiative for Cybersecurity Careers and Studies, n.d., https://niccs.us-cert.gov/awareness/cybersecurity-101.
4. White House, Office of the Press Secretary, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," May 29, 2009, https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure
5. Edward Amoroso, Cyber Security (Summit, NJ: Silicon Press, 2007), 58-59.
6. Ibid., 14-15.
7. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Harper Collins, 2012), 246.
8. Ibid., 170.
9. "Explore Terms: A Glossary of Common Cybersecurity Terminology," National Initiative for Cybersecurity Careers and Studies, n.d., http://niccs.us-cert.gov/glossary.
10. CERT Insider Threat Center (Carnegie-Mellon Univ.), http://csrc.nist.gov/news_events/HIPAA-May2011_workshop/presentations/day2_HIPAA-conference2011-Insider-Threat.pdf.
11. White House, Office of the Press Secretary, "Annual Report to Congress: Federal Information Security Management Act," February 27, 2015, 6,https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.
12. Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Cyber Conflict Studies Association, 2013), 165.
13. Hewlett-Packard, "Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape," August 2014, http://h30499.www3.hp.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf.
14. Ibid.
15. Healey, A Fierce Domain, 174.
16. Ibid., 194.
17. Ibidem, 167-169. Also see, http://www.wsj.com/articles/SB124027491029837401.
18. Ibidem, 75-77.
19. Ibidem, 212, 219.
20. Henry Dalziel, "The Four Amigos: Stuxnet, Flame, Gauss, and Duqu," *Concise*, February 11, 2013, https://www.concise-courses.com/security/stuxnet-flame-gauss-duqu/.
21. Healey, A Fierce Domain, 220.
22. Frederick Kagan and Tommy Stiansen, "The Growing Cyber Threat from Iran," American Enterprise Institute, April 2015, https://www.aei.org/wp-content/uploads/2015/04/Growing-Cyberthreat-From-Iran-final.pdf.
23. Pierluigi Paganini,"RasGas, new cyberattack against an energy company," *Security Affairs*, August 31, 2012, http://securityaffairs.co/wordpress/8332/malware/rasgas-new-cyber-attack-against-an-energy-company.html
24. Benjamin Elgin and Michael Riley, "Now at the Sands Casino: An Iranian Hacker in Every Server," Bloomberg, December 12, 2014, http://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas.
25. Kim Zetter, "Sony Got Hacked Hard," *Wired*, December 3, 2014, http://www.wired.com/2014/12/sony-hack-what-we-know/.
26. Ellen Nakashima, "Hacks of OPM Database Compromised 22.1 Million People," *Washington Post*, July 9, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.
27. James R. Clapper, Statement for the record before the Senate Armed Services Committee, February 9, 2016, http://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.
28. Senior Colonel Wang Baocun and Li Fei, "Information Warfare," FAS.org, June 13 and 20, 1995, http://fas.org/irp/world/china/docs/iw_wang.htm.
29. Bradley Raboin, "Corresponding Evolution: International Law and the Emergence of Cyber Warfare," *Journal of the National Association of the Administrative Law Judiciary* 31, no. 2, Fall 2011, http://docplayer.net/6875528-Corresponding-evolution-international-law-and-the-emergence-of-cyber-warfare.html.
30. U.S. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015*, April 7, 2015, 37, http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf.
31. "China to Speed Up Full Military IT Application: Hu," Xinhua, November 8, 2012, http://news.xinhuanet.com/english/special/18cpcnc/2012-11/08/c_131959900.htm.
32. "Full Text: China's Military Strategy," Xinhua, May 26, 2015, http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm.
33. Desmond Ball, "Security Trends in the Asia-Pacific Region," Strategic and Defence Studies Centre *Working Paper* no. 380, November 2003, http://ips.cap.anu.edu.au/sites/default/files/WP-SDSC-380.pdf.
34. Desmond Ball, "China's Cyber Warfare Capabilities," *Security Challenges* 7, no. 2, Winter 2011, http://indianstrategicknowledgeonline.com/web/china%20cyber.pdf.
35. Hannah Beech, "Meet China Newest Soldiers: An Online Blue Army," *Time*, May 27, 2011, http://world.time.com/2011/05/27/meet-chinas-newest-soldiers-an-on-line-blue-army/. Leo Lewis, "China's Blue Army of 30 Computer Experts Could Deploy Cyber Warfare on Foreign Powers," *The Australian*, May 27, 2011, http://www.theaustralian.com.au/business/technology/chinas-blue-army-could-conduct-cyber-warfare-on-foreign-powers/story-e6frgakx-1226064132826.
36. Bill Gertz, "Cheers to Good Frenemies! China Investing in Cyberwarfare Superiority," *Washington Times*, April 1, 2015, http://www.washingtontimes.com/news/2015/apr/1/china-invests-cyberwarfare-compete-us-military/?page=all.
37. Eric Heginbotham et al., *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power 1996-2017* (Santa Monica: RAND, 2015), http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR392/RAND_RR392.pdf.
38. "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, February 18, 2013, http://intelreport.mandiant.com/Mandiant_ APT1_Report.pdf.
39. Bryan 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, October 9, 2009, http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf.
40. Jamie M. Ellis, "Chinese Cyber Espionage: A Complementary Method to Aid PLA Modernization," Naval Postgraduate School thesis, December 2015, 78, https://www.hsdl.org/?view&did=790444.
41. Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation."
42. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015*, 37.
43. Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," *Wall Street Journal*, April 8, 2009, http://www.wsj.com/articles/SB123914805204099085.
44. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015*, 39.
45. Clapper, Statement for the record before the Senate Armed Services Committee.
46. Hewlett-Packard, "Profiling an Enigma."
47. Gabi Siboni and Sami Kronenfeld, "Developments in Iranian Cyber Warfare, 2013-2014," Institute for National Security Studies Insight, April 3, 2014, http://www.inss.org.il/index.aspx?id=4538&articleid=6809.
48. Ibid.
49. Ilan Berman, testimony before the House of Representatives Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence, February 11, 2016, 7, http://docs.house.gov/meetings/HM/HM05/20160211/104455/HHRG-114-HM05-Wstate-BermanI-20160211.pdf.
50. Cory Bennett, "Iran Has Boosted Cyber Spending Twelvefold," *The Hill*, March 23, 2015, http://thehill.com/policy/cybersecurity/236627-iranian-leader-has-boosted-cyber-spending-12-fold.

REFERENCES

51. Nart Villeneuve et al., "Operation Safron Rose," FireEye, 2013, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf.
52. "Structure of Iran's Cyber Warfare," *BBC Persian*, n.d., http://nligf.nl/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf.
53. Michael A. Riley and Jordan Robertson, "Iran-Backed Hackers Target Airports, Carriers: Report," *Bloomberg Business*, December 2, 2014, http://www.bloomberg.com/news/articles/2014-12-02/iran-backed-hackers-target-airports-carriers-report.
54. "Structure of Iran's Cyber Warfare."
55. Ibid.
56. Riley and Robertson, "Iran-Backed Hackers Target Airports, Carriers: Report."
57. Cylance, *Operation Cleaver*, Cylance, December 2014, http://www.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf.
58. Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival* 55, no. 2, April-May 2013, 81-96, http://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272.
59. Tracy Connor, Stephanie Gosk and Tom Winter, "Iranian Hackers Claim Cyber Attack on New York Dam," *NBC News*, December 23, 2015, http://www.nbcnews.com/news/us-news/iranian-hackers-claim-cyber-attack-new-york-dam-n484611. See also David E. Sanger, "U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam," *New York Times*, March 24, 2016, http://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html?_r=0.
60. Clapper, statement for the record before the Senate Armed Services Committee.
61. Hewlett-Packard, "Profiling an Enigma."
62. Ibid. See also Martyn Williams, "What We Know About North Korea's Cyberarmy," *PC World*, December 19, 2014, http://www.pcworld.com/article/2861692/what-we-know-about-north-koreas-cyberarmy.html.
63. Devin Dwyer, "President Obama Sanctions North Korea after Sony Cyber Attack." *ABC News*, January 2, 2015, http://abcnews.go.com/Politics/obama-sanctions-north-korea-sony-cyberattack/story?id=27965524.
64. Hewlett-Packard, "Profiling an Enigma."
65. Clapper, statement for the record before the Senate Armed Services Committee.
66. NATO Cooperative Cyber Defense Center of Excellence, "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space," 2011, https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf.
67. James R. Clapper, statement for the record before the Senate Armed Services Committee, September 29, 2015, http://www.armed-services.senate.gov/imo/media/doc/Clapper_09-29-15.pdf.
68. Ward Carroll, "Russia's Cyber Forces," DefenseTech, May 27, 2008, http://defensetech.org/2008/05/27/russias-cyber-forces/.
69. David Smith, "How Russia Harnesses Cyberwarfare," American Foreign Policy Council *Defense Dossier* iss. 4, August 2012, http://www.afpc.org/files/august2012.pdf.
70. David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf
71. Paul Shinkman, "Reported Russian Cyber Attack Shuts Down Pentagon Network," *U.S. News & World Report*, August 6, 2015, http://www.usnews.com/news/articles/2015/08/06/reported-russian-cyber-attack-shuts-down-pentagon-network.
72. Evan Perez and Shimon Prokupecz, "How the US Thinks Russians Hacked the White House," *CNN*, April 8, 2015, http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/.
73. United States Cyber Command, "Cyber Guard 15 Fact Sheet," n.d., http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Cyber_Guard_15_Fact_Sheet_010715_f.pdf.
74. NIST Cybersecurity Framework, "Overview," n.d., http://www.nist.gov/cyberframework/.
75. U.S. Department of Defense, "The Department of Defense Cyber Strategy," April 2015, http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
76. United States Strategic Command, "Fact Sheet: U.S. Cyber Command," n.d., https://www.stratcom.mil/factsheets/2/Cyber_Command/
77. U.S. Department of Defense, "The Department of Defense Cyber Strategy."
78. Andrea Peterson, "The NSA Has its Own Team of Elite Hackers," *Washington Post*, August 29, 2013 https://www.washingtonpost.com/news/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers/.
79. Ibid.
80. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, March 11, 2014, http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
81. Ellen Nakashima, Greg Miller, and Julie Tate, "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," *Washington Post*, July 19, 2012, https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.
82. U.S. Government Accountability Office, "Cybersecurity," n.d., http://www.gao.gov/key_issues/cybersecurity/issue_summary.
83. U.S. Department of Homeland Security, "Critical Infrastructure Sectors," October 27, 2015, https://www.dhs.gov/critical-infrastructure-sectors.
84. The White House, "Cybersecurity," n.d., https://www.whitehouse.gov/issues/foreign-policy/cybersecurity
85. Debra Werner, "Hacking Cases Make Security a Selling Point for Commercial Providers," *Space News*, March 19, 2012, http://spacenews.com/hacking-cases-make-security-selling-point-commercial-providers/.
86. U.S. Department of Justice, "Administrator of VisionTech Components, LLC Sentenced to 38 Months in Prison for Her Role in Sales of Counterfeit Integrated Circuits Destined to U.S. Military and Other Industries," October 25, 2011, https://www.justice.gov/archive/usao/dc/news/2011/oct/11-472.html.
87. White House, Office of the Press Secretary, "Fact Sheet: Cybersecurity National Action Plan," February 9, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.
88. Ibid.
89. Damian Paletta, "NSA Chief Says U.S. at 'Tipping Point' on Cyberweapons," *Wall Street Journal*, January 21, 2016, http://www.wsj.com/articles/nsa-chief-says-u-s-at-tipping-point-on-cyberweapons-1453404976.
90. Ibid.
91. "Rules Committee Print 114-39 Text of House Amendment #1 to the Senate Amendment to H.R. 2029, Military Construction and Veterans Affairs and Related Agencies Appropriations Act, 2016," United States House of Representatives, December 15, 2015, http://docs.house.gov/billsthisweek/20151214/CPRT-114-HPRT-RU00-SAHR2029-AMNT1final.pdf.
92. "Congress Passes Four Cybersecurity Bills," *National Law Review*, December 13, 2014, http://www.natlawreview.com/article/congress-passes-four-cybersecurity-bills.
93. "H.R.2592 - Cybersecurity Workforce Assessment Act," United States House of Representatives, December 18, 2014, https://www.congress.gov/bill/113th-congress/house-bill/2952.
94. James R. Clapper, statement for the record before the House Permanent Select Committee on Intelligence, September 10, 2015, http://www.dni.gov/files/documents/HPSCI%2010%20Sept%20Cyber%20Hearing%20SFR.pdf.
95. Scott Maucione, "White House Finally Acquiesces to Congress on Cyber Deterrence Policy," *Federal News Radio*, December 29, 2015, http://1yxsm73j7aop3quc9y5i-faw3.wpengine.netdna-cdn.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf

AFPC INFORMATION

For over three decades, the American Foreign Policy Council (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.

About The Defense Technology Program A revolution is taking place in the nature of warfare. The proliferation of ballistic missiles and weapons of mass destruction has given rogue states and terrorist groups unprecedented access to potentially devastating capabilities, while space and cyberspace have emerged as distinct new arenas of strategic competition. The American Foreign Policy Council's work in these areas is aimed at helping U.S. officials understand and respond to this new, and increasingly complex, threat environment.

For more information about the program, please contact Richard Harrison, Director of Operations and Defense Technology Programs at Harrison@afpc.org.

509 C Street NE | Washington, D.C. 20002 | 202.543.1006
www.afpc.org