

NARCO SUBS • TRACKING THE TALIBAN • HEZBOLLAH • DEMOGRAPHIC WARFARE

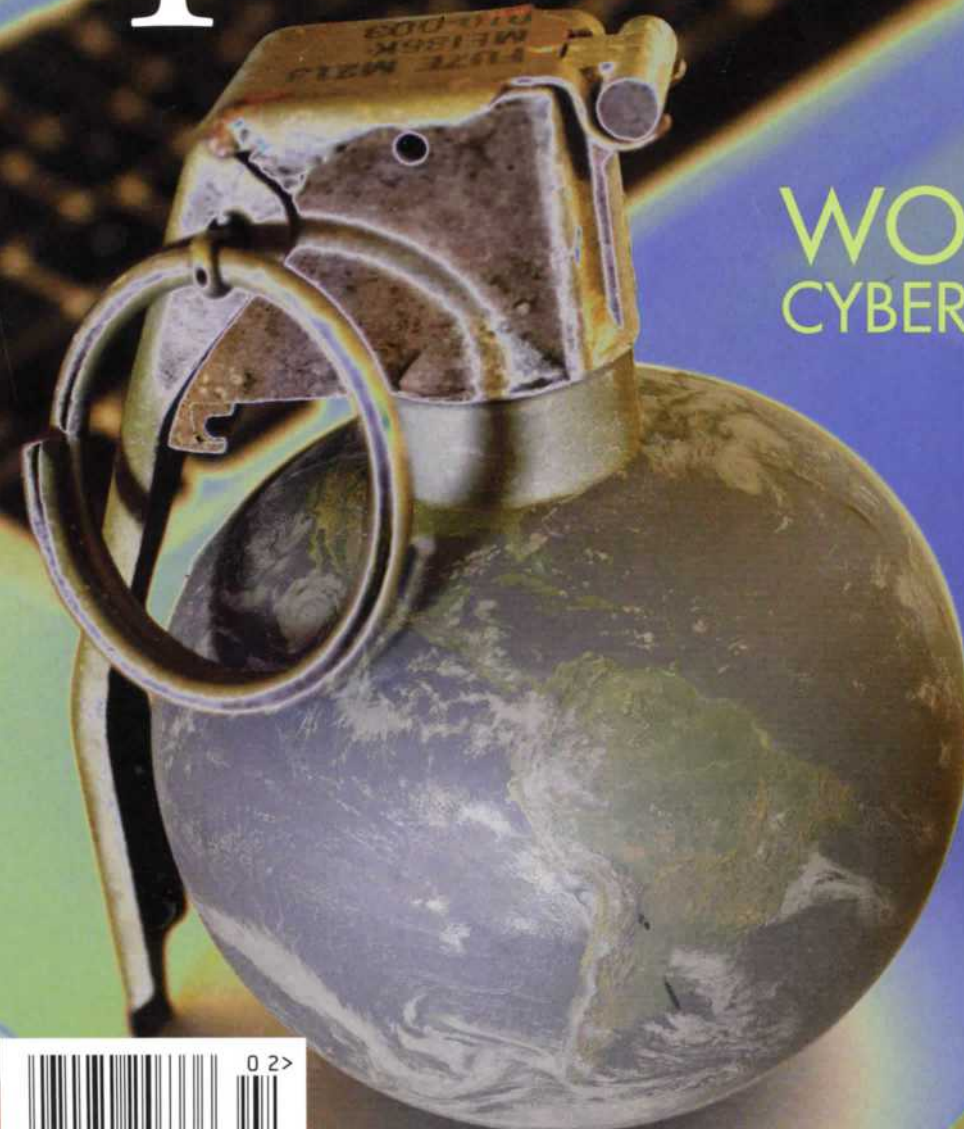
Journal for Law Enforcement, Intelligence & Special Operations Professionals

The Counter Terrorist

FEBRUARY/MARCH 2013

VOLUME 6 • NUMBER 1

WORLD
CYBER WAR

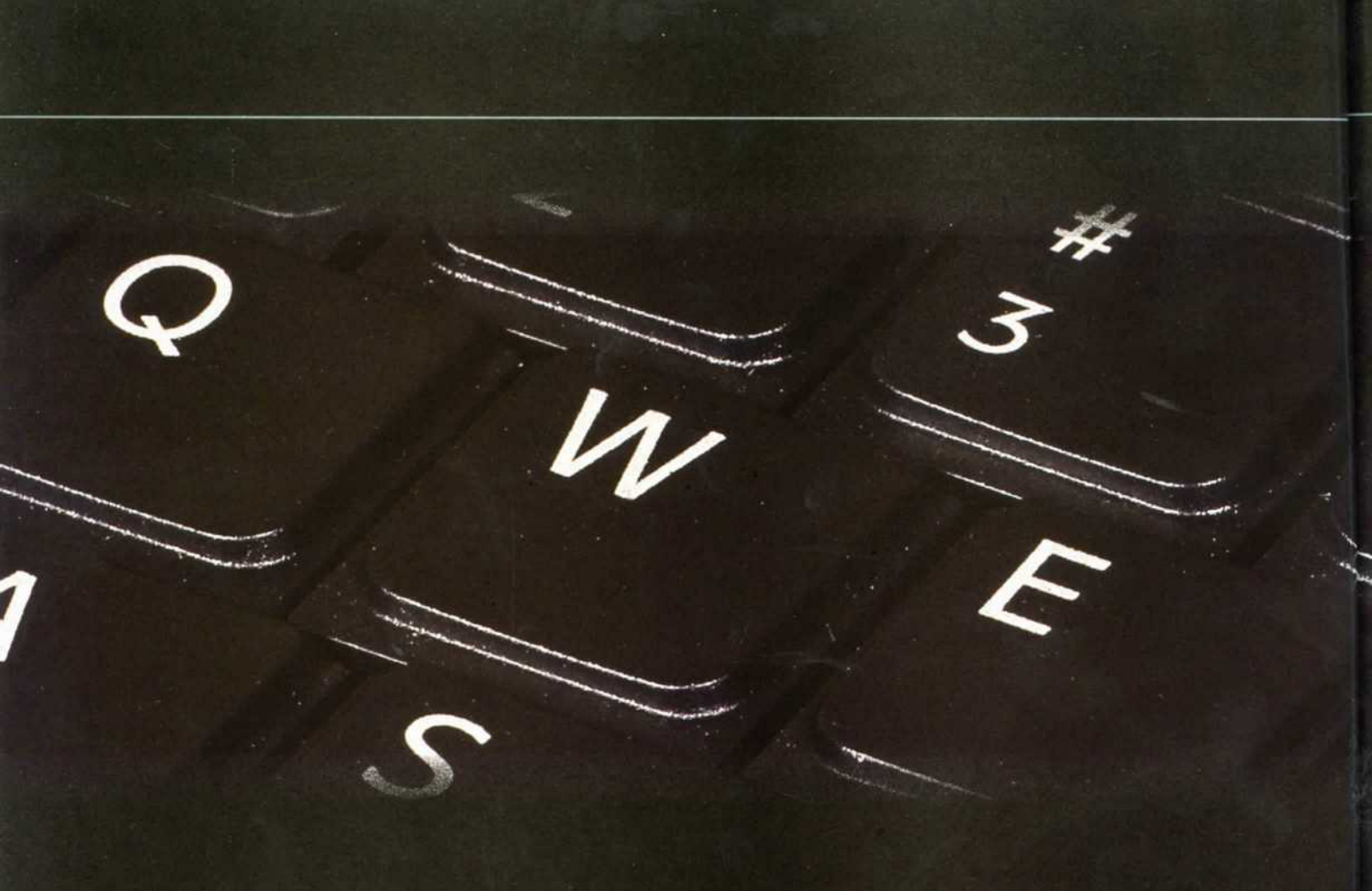


FEBRUARY/MARCH 2013
USA/CANADA \$5.99

INTERNATIONAL
EDITION

An SSI® Publication

www.thecounterterroristmag.com



WORLD CYBER WAR

By Chris Mark



Dr. Bruce Schneier has stated that "Cyberwar is certainly not a myth. But you have not seen it yet, despite the attacks."¹ He astutely states, "The biggest problems in discussing cyberwar are the definitions."

Many people tend to abide by a very binary, traditional (and outdated) Western view of war and warfare, which has historically been defined by direct, kinetic actions. many "experts" are resistant to the notion that the United States is engaged in a war with its adversaries despite the fact that other countries and non-state belligerents have stated they are waging war against the United States and its allies.

"A single rumor or scandal that results in fluctuation in the enemy country's exchange rates... can be included in the ranks of new concept weapons." –Unrestricted Warfare²

On September 6, 2007, a suspected Syrian nuclear facility being built by North Koreans was bombed and destroyed by Israeli F-15s. While the story was disputed by Syria and North Korea, the United States took the unusual step of releasing clandestine video of the

facility that left little doubt as to the nature of the construction. To many, this is simply another banal act in a long line of bombings, invasions, and military activities by adversaries. Looking more closely, however, it is more profound. As can be expected of any country building a nuclear facility in violation of the United Nation's Non Proliferation Pact, Syria had invested significantly (billions of US dollars) in advanced Russian air defense



*Before and after picture of building struck during Operation Orchard in Syria.
Photo: US government*

systems. How then did Israel manage to circumvent these defense systems? According to Richard Clarke: "What appeared on the radar screen is what the Israelis had put there, an image of nothing."³

There are three prevailing theories as to how the mission was accomplished: The first is that electronic jamming systems were used to inject malicious code in the radar receivers in much the same way a virus or worm is installed on a computer over the Internet. The second theory is that the Russian computer code used in the radar facilities had been compromised and a "backdoor" inserted into the code, allowing agents to remotely control the radar system. The final option was that the fiber optic cable used to transmit information had been tapped and malicious instructions inserted into communications.

Regardless of the method, the Syrians were unable to identify the planes as they were approaching the facility for a bombing run.⁴ This was neither the first

nor last time cyberattacks were used in furtherance of military objectives:

- In 2004, before the invasion of Iraq, hackers reportedly penetrated the secure, "closed loop" private network of the Iraqi army. Iraqi officers received emails on the Defense Ministry Email System warning of the impending attack and providing directions for surrendering. Many Iraqi officers heeded the warning and lined their tanks up in anticipation of the Allied invasion.⁵

- In 2006, several months after attempting to hack the Bureau of Industry and Security (BIS), hackers successfully penetrated US Naval War College systems. The attack was traced back to China and was the third identified attack by the Chinese against DOD systems in 2006.⁶

- In 2008, Russia invaded the Republic of Georgia over a dispute in two Ossetian territories. Before the invasion, the Georgian government's websites were attacked with Distributed Denial of Service Attacks (DDOS) and defacements

in which the Georgian leader was portrayed as Adolf Hitler.⁷

- On April 21, 2009, the US Department of Defense acknowledged that 1.5 terabytes of data on the F35 Joint Strike Fighter had been stolen by Chinese hackers. The theft of this data represented over \$300 billion in research and development operations. As an advanced fighter has little use in the civilian market, this is a clear example of military technology being stolen to advance the interests of a foreign nation.⁸

On December 4, 2011, an American RQ-170 Sentinel unmanned aerial vehicle (UAV) was captured near the city of Kashmar in northeastern Iran. The Iranian government announced that the UAV was brought down by a cyberwar unit that commandeered the aircraft and landed it.

In 2012, US Natural Gas Pipeline companies have been hit with continual cyberattacks widely attributed to the same Chinese hackers that were responsible for the compromise of RSA.⁹

To understand the significance of these attacks and why they represent acts of war, it is important to have a working definition of the concepts of war, cyberwar, and cyberspace.

According to Prussian military strategist Carl von Clausewitz, war:

*"is nothing but a duel on an extensive scale... we shall do so best by supposing to ourselves two wrestlers. Each strives by physical force to compel the other to submit to his will... War therefore is an act of violence to compel our opponent to fulfill our will"*¹⁰

From the early 20th century, wars have been fought in the three primary domains of land, sea, and air. In 1957, the United States added a fourth warfighting domain—space.¹¹ By 2007, cyberspace was officially recognized by the US Air Force as a warfighting domain. This fifth

domain is of particular interest.¹² Within the first four domains, von Clausewitz's definition of war was widely regarded as appropriate, as violence can be applied quite effectively to force an opponent to "submit." With the recognition of more domains, however, it is necessary to refine the definition of war. It is also necessary to acknowledge that nation states are not the only practitioners of warfare.

There are two commonly understood applications for the concept of cyberwar. First is to make a conventional attack easier by disabling the enemy's defenses. The second use of cyberwar is to send propaganda to demoralize the enemy.¹³

In 2008, Homeland Security Presidential Directive 23, "Cyber Security Policy" was signed by President George W. Bush. The directive defined cyberspace as:

*"The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."*¹⁴

Interestingly, it is difficult to find an official definition of "cyberwar." According to Richard Clarke, "cyberwarfare" is defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."¹⁵ This definition harkens back to von Clausewitz and is not consistent with how adversaries view cyberwar. As Schneier said, "The biggest problems in discussing cyberwar are the definitions."

"THE WAR GOD'S FACE HAS BECOME INDISTINCT"

— UNRESTRICTED WARFARE ¹⁶

To highlight the differing views of war and warfare, one need only to look to China. China, as an acknowledged Western adversary, has been on the forefront of cyber-espionage efforts against the West and has embraced an evolving concept of war since the late 1980s. In 1988, China's information warfare theorist, Dr. Shen Weiguang, posited that:

"Virus-infected microchips can be put in weapon systems," or "An arms manufacturer can be asked to write a virus into software, or a biological weapon can be embedded into the computer system of an enemy nation and then activated as needed... Preparation for a military invasion can include hiding self-destructing microchips in systems designed for export."

Dr. Shen recognized that these tactics, if carried out systematically, could have


INSTANTLY MAP YOUR TACTICAL TEAM AND SHARE LIVE VIDEO AND INFORMATION

GPS track, map and connect tactical teams, snipers, robots, and surveillance devices. Share live video, photos, and text on iPads/iPhones and laptops.

Want to see what your sniper sees? Click on his icon to see.

Suspect photo? Send it to everyone on the system.

COMMANDLINK O·V·E·R·W·A·T·C·H



Actual screen shots


CommandLink Overwatch. A powerful, affordable tactical management system.

- ◆ All iDevices/robots appear as map icons
- ◆ Click teammember icon to access data
- ◆ Receive live video from robots or cams
- ◆ Push text, pics, unlimited notes to users
- ◆ Drop or set placemark pins
- ◆ Military encryption

Lithos Robotics

www.lithosrobotics.com

716.832.4600



... "destroy the enemy's political, economic, and military information infrastructures, and, perhaps, even the information infrastructure for all of society."

profound strategic implications. They could, according to Shen, "destroy the enemy's political, economic, and military information infrastructures, and, perhaps, even the information infrastructure for all of society." Shen believed this would allow China to achieve the greatest military objective. To "destroy the enemy's will to launch a war or wage a war."¹⁷

Advancing this theory, in 1995, Major General Wang Pufeng, former Director of the Strategy Department of the Academy of Military Sciences, wrote:

*"In the near future, information warfare will control the form and the future of war. We recognize this developmental trend of information warfare and see it as a driving force in the modernization of China's military and combat readiness."*¹⁸

Adding to Dr. Shen and General Wang's positions, the Chinese government sponsored research by People's Liberation Army (PLA) Colonels Qiao Liang and Wang Xiangsui. In the seminal 1999 work titled *Unrestricted Warfare* the authors succinctly state China's evolving definition of war when they say:

*"If we acknowledge that the new principles of war are no longer 'using armed force to compel the enemy to submit to one's will,' but rather are 'using all means including armed force and non-armed force, military and non-military, lethal and non-lethal means to compel the enemy to accept one's interests.'"*¹⁹

A more evolved definition of cyber weapons may also be seen in *Unrestricted Warfare*.

"As we see it, a single man-made stock-market crash, a single computer virus invasion, or a single rumor or scandal that results in a fluctuation in the enemy country's exchange rates or exposes the leaders of an enemy country on the Internet,

*all can be included in the ranks of new-concept weapons."*²⁰

By 1999, the Chinese had already adopted a theory of warfare that embraced means of "compelling the enemy to accept one's interests." In short, China has redefined the concept of war and warfare to include what they call "semi-warfare, quasi-warfare, and sub-warfare, that is, the embryonic form of another kind of warfare." While many "experts" in the United States may dispute that their country is at war, few leaders in China are likely to share that perspective.

"THE UNITED STATES IS UNDER ATTACK"

— 2011; US HOUSE OF REPRESENTATIVES

While some would argue that the United States has been slow to react, China's actions have not gone unnoticed. On April 15, 2011, the United States Congress House Committee on Foreign Affairs held hearings titled *Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology*. The opening remarks state clearly the United States position:

"The Chinese Communist Government has defined us as the enemy. It is buying, building and stealing whatever it takes to contain and destroy us. Again, the Chinese Government has defined us as the enemy. Chinese cyber-attacks on US assets now number in the thousands every year."

This statement is the first public acknowledgement that the United States views Chinese actions as aggressive. It is important to note that cyber warfare has been integrated into the formal order of battle of the conventional military forces of the PLA. While some may view cyber-espionage and data theft in purely commercial terms, it is

important to understand that Chinese strategy considers cyber-espionage as a critical component of their cyber warfare strategy. As detailed in the aforementioned hearings:

"The economics of cyber theft is simple: Stealing technology is far easier and cheaper than doing original research and development. It is also a far less risky way to spy than historic cloak and dagger economic espionage."²¹

The Chinese do not simply engage in cyber-espionage for corporate gain, rather the Chinese government supports cyber-espionage in furtherance of national goals.²² The key point to understanding the objective of cyber-espionage by the People's Republic of China (PRC), whether companies, individuals, or directly government, is to understand

their National Security "16 character policy." The 16 Character Policy translates to "Give priority to military products." In short, cyber-espionage and data theft benefits the Chinese government first and foremost.²³

The PRC relentlessly engages in cyber-espionage activities against every country in which the PRC has an interest. Using "cyber militias" consisting of patriotic hackers and more formal military units such as the Special Tactical Reconnaissance Units of the PLA, the Chinese engage in ongoing cyber-espionage with the objective of supporting military objectives.²⁴ International companies are now subject to continuous probes seeking any and all manner of information, whether military, commercial, or political. China has

embraced the idea that "the richest source of power to wage war lies in the masses of the people."²⁵ With almost 2 billion people, they have a significant power to wage war. In 2006, one patriotic group, the Red Hacker Alliance, alone counted more than 300,000 members.²⁶

**"A RAPID, POWERFUL
TRANSITION TO
THE ATTACK—THE
GLINTING SWORD
OF VENGEANCE—IS
THE MOST BRILLIANT
MOMENT OF DEFENSE."**

— CARL VON CLAUSEWITZ²⁷

In October 2012, President Barack Obama signed *Presidential Policy Directive*²⁸. This is an update to a 2004



Mini-CALIBER®

SWAT ROBOT

THE FIRST ONE IN

The ICOR Mini-CALIBER® is an affordable SWAT robot that provides fast action for area search and clearance, reconnaissance, crisis negotiation, and package delivery.

Make it your first eyes and ears on high threat targets!

ICOR stands behind our robots with a 2 year warranty and unlimited technical support.

Contact ICOR for full technical specifications and request a demonstration.

Visit www.icortechnology.com to see our full line of Tactical equipment.





800.542.5243

www.southernpoliceequipment.com

www.southernpoliceequipment.com

NEW CATALOG NOW AVAILABLE

**100% Woman Owned
Small Business**



**Over 11,000 Products
on GSA ADVANTAGE
GS-07F-0273T**



**Boots & Gas
Mask Carriers**



**New
Catalog
Available**



Night Optics



**Training
Simulators**



**Green
Laser
Illuminators**



**Send All GSA Inquiries To:
walter@
southernpoliceequipment.com**



A Tactical Tomahawk Cruise Missile launches from the forward missile deck aboard the guided-missile destroyer USS Farnagut (DDG 99) during a training exercise. Photo: Mass Communication Specialist 1st Class Leah Stiles/Released

directive signed by then President George W. Bush. While classified, the Directive reportedly outlines, for the first time, that the United States could engage in offensive cyber operations. As stated by a senior administration official:

*"What it does, really for the first time, is it explicitly talks about how we will use cyber-operations," further- "Network defense is what you're doing inside your own networks. ... Cyber-operations is stuff outside that space, and recognizing that you could be doing that for what might be called defensive purposes."*²⁸

While it is important to understand that the United States, as an open and interconnected society, clearly has some vulnerabilities, it also has some claws with which to defend national interests. Several public examples highlight

the United States' own ability to wage cyberwar.

According to *The New York Times*,²⁹ former President Bush initiated a classified program, continued by President Obama, known as "Olympic Games" that included sophisticated attacks on the computer systems used to run Iranian nuclear enrichment facilities. The public became aware of the program in the summer of 2010 after a virus, known as Stuxnet, escaped from the facility and began infecting systems throughout the world. Stuxnet was designed to send commands to the centrifuges, which caused them to spin abnormally, thereby destroying the centrifuges. According to Kaspersky Labs, the sophistication of the Trojan indicates that it was built by a nation state. The most likely candidates, they say, were the

United States and Israel.

After the discovery of Stuxnet came the discovery of the Duqu virus, which contains ninety-five percent of the same code as Stuxnet but is much more sophisticated. Following Duqu was the Flame virus. Called by a researcher "the most complex piece of malicious software discovered to date," Flame was designed to capture data and also to change computer setting and turn on integrated microphones to record what is being said in a room. Kapersky Labs discovered the virus, which had been lurking undetected inside thousands of computers for as long as five years. According to Kapersky, the countries with the most infections include Iran, followed by the Israel/Palestine area, Syria, and Sudan. According to Kapersky Senior Researcher

Roel Schouwenberg, "The virus contains about 20 times as much code as Stuxnet, which attacked an Iranian uranium enrichment facility, causing centrifuges to fail."⁵⁰

When considering whether cyberwar is at hand, it is important to consider the position of adversaries. It is easy to fall into a state of complacency because the actions of one's adversaries don't look like traditional warfare. It appears that the Chinese, Russians, North Koreans, Iranians, and others (including non-state actors) are focused on achieving strategic goals using non-traditional warfare. The PRC, in particular, gives insight into its approach to warfare in *Unrestricted Warfare*. While many "experts" ignore the significance of cyberattacks, they are a continuing rain of blows. One cannot

afford to discount the capabilities of an enemy that does not fight conventionally just because conventional wisdom holds that his capabilities are "inferior." •

ABOUT THE AUTHOR

Mr. Mark is the founder of Mark Consulting Group, Inc. He is a data security and risk professional. He has consulted for numerous Fortune 500 companies and publishes the blog: www.GlobalRiskInfo.com.

ENDNOTES

¹Bruce Schneier, "Cyber war: Myth or Reality?" *Freedom from Fear Magazine*, http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=315:cyberwar-myth-or-reality&catid=50:issue-7&Itemid=187.

²Wiangsui Qiao Liang and Wang, *Unrestricted Warfare*, (Beijing: PLA Literature and Arts Publishing House; 1999).

³Richard A. Clarke, and Robert K. Knake. *CYBERWAR*. (New York: Harper Collins, 2010) 5.

⁴Clarke and Knake, *CYBERWAR*, 9-10

⁵Clarke and Knake, *CYBERWAR*, 9-10

⁶"Third Chinese Hack Attack This Year," Strategy Page, December 4, 2006, <http://www.strategypage.com/htm/htw/articles/20061204.aspx>.

⁷Clarke and Knake, *CYBERWAR*, 19.

⁸Christopher Goins, "Chinese Hackers Stole Plans for America's New Joint Strike Fighter Plane, Says Investigations Subcommittee Chair," *CNS News*, April 25, 2012, <http://cnsnews.com/news/article/chinese-hackers-stole-plans-america-s-new-joint-strike-fighter-plane-says-investigations>.

⁹Mark Clayton, "Exclusive: Potential China Link to Cyberattacks on Gas



WWW.FLASHBANGPOLE.COM

