Are Cyber Weapons Effective Military Tools?

Emilio Iasiello

Cyber-attacks are often viewed in academic and military writings as strategic asymmetric weapons, great equalizers with the potential of leveling the battlefield between powerful nations and those less capable. However, there has been little evidence to suggest that cyber-attacks are a genuine military option in a state-on-state conflict. In instances of actual military operations (e.g., Afghanistan, Georgia, Iraq, and Israel/Gaza), there is little accompanying evidence of a military conducting cyber-attacks against either a civilian or military target. Given that some of the nation states that have been involved in military conflict or peacekeeping missions in hostile areas are believed to have some level of offensive cyber capability, this may be indicative. More substantive examples demonstrate that cyber-attacks have been more successful in non-military activities, as they may serve as a clandestine weapon of subterfuge better positioned to incapacitate systems without alerting the victims, veiling the orchestrator's true identity via proxy groups and plausible deniability. Consequently, this paper provides a counter argument to the idea that cyber tools are instrumental military weapons in modern day warfare; cyber weapons are more effective options during times of nation state tension rather than military conflict, and are more serviceable as a signaling tool than one designed to gain military advantage. In situations where state-on-state conflict exists, high value targets that need to be neutralized would most likely be attacked via conventional weapons where battle damage assessment can be easily quantified. This raises the question: are cyber weapons effective military tools?

Key words: cyber-attack, cyber weapons, state-on-state conflict.

Emilio Iasiello has more than 12 years' experience as a strategic cyber intelligence analyst, supporting US government civilian and military intelligence organizations, as well as a private sector company providing cyber intelligence to Fortune 100 clients.

Terminology

There is no international consensus on the definitions for "cyber-attack" and "cyber weapon." However, it can be agreed that these terms refer to the execution of malware with the objective of denying, disrupting, degrading, destroying, or manipulating information systems or the information resident on them. Taking this into consideration, the following definitions have been adopted for this paper:

- **Cyber-Attack**: "actions taken through computer networks designed to deny, degrade, disrupt, or destroy an information system, an information network, or the information resident on them."
- **Cyber Weapon**: this paper accepts the definition created by Thomas Rid and Peter McBurney: "a computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings."[1]Examples include distributed denial-of-service (DDoS) attacks and the insertion of malware designed to destroy information systems or the information resident on them.

Cyber as an Asymmetric Weapon

Military writings on cyber warfare – a subset of the larger information warfare umbrella – frequently cite critical infrastructures as key targets for military action during times of conflict, as they are seen as enablers of a nation state's military capabilities. The U.S. Department of Homeland Security defines critical infrastructures as "the assets, systems, and networks, whether physical or virtual, 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."[2] Cyber-attacks in the information environment are important facets of force projection, particularly against soft targets such as communication systems, ports, airports, staging areas, civilian populations, critical infrastructure, and economic centers. In this context, cyber weapons are an ideal embodiment of an asymmetric strategy: the more technically sophisticated a powerful nation's information infrastructure, the more vulnerable it is to cyber-attacks.

Nation State Writings on Information Warfare

The fundamental principle of an asymmetric strategy is to convert the adversary's perceived strength into its weakness. Certainly, in no other area

is this best exemplified than in the cyber domain where the very software and hardware complexities that increase military and societal effectiveness and productivity are also fraught with exploitable vulnerabilities. Academics and military theorists have been contemplating information warfare for many years. In the United States, the earliest reference to information warfare can be attributed to Dr. Tom Rona in the 1970s.[3] The first military adoption of this term was in 1992, when the U.S. Department of Defense published a more formalized definition of information warfare in its classified TS3600.1 policy document.[4] The U.S. military altered the definition throughout the years but the term had become part of its lexicon even if there were no formalized strategies to guide implementation during wartime.

The U.S. was not alone in cultivating progressive thinking on the nature of information warfare and how it could be leveraged for maximum effect. Chinese and Russian military theorists also wrote extensively on the topic. While initial writings seemed more of a mirroring of earlier published material, they did contemplate how such tools could be used as an implement of war. Despite cultural nuances, all agreed on the potential of information warfare as a weapon to bridge the differential gap between superior and inferior forces providing the latter with the means to strike without risking full force-on-force engagement. "Asymmetric" highlights this sentiment, and as one writer described it, is "roughly akin to the Japanese martial art of jujutsu, which is based on the idea that an opponent's strength and energy may be used against him rather than directly opposed with strength of one's own."[5] Unlike nuclear weaponry that requires significant resources and capability for production and management, information war and its instruments are easily accessible to the masses.

Chinese Writing on Information Warfare

The earliest Chinese writing on information warfare is probably the book entitled "Information Warfare," published in 1985 which had later become an article in the Liberation Army Daily.[6] However, it wasn't until Operation Desert Storm that Chinese theorists saw a military using advanced technology to defeat an opponent. In 1995, People's Liberation Army (PLA) Major General Wang PuFeng wrote "The Challenge of Information Warfare" frequently referencing U.S. information warfare efforts against Iraq.[7] Another writer saw this battle as a "great transformation" where information and command and control revolutionized the battlefield.[8]

Scholars considered "information dominance" a key concept to obtaining victory in future wars.

Two Chinese military doctrinal writings, the *Science of Strategy* and the *Science of Campaigns*, acknowledge information warfare as an important military tool for countering a superior adversary's informational and technological advantages. Influential military strategists from prominent Chinese military academies and schools have suggested that China's military should implement cyber or precision-weapon attacks against such critical infrastructure targets as ports and airports. Indeed, many of the more authoritarian writings regarding Chinese military thought advocate this course of action. In the *Science of Campaigns*, the author posits that information warfare is to be used:

> At the critical time and region related to overall campaign operations, to cut off the enemy's ability to obtain, control, and use information, to influence, reduce, and even destroy the enemy's capabilities of observing, decision-making, and commanding and controlling troops, while we maintain our own ability to command and control in order to seize information superiority, and to produce the strategic and campaign superiority, creating conditions for winning the decisive battle.

China's Integrated Network Electronic Warfare (INEW) theory places peacetime and wartime computer network attack and electronic warfare under one authority. Its mission is to disrupt the opponent's ability to process and use information. The strategy is characterized by the combined employment of network tools and electronic warfare weapons against an adversary's information systems in the early phases of a conflict.[9] According to Chinese thought, the strength of such attacks lies in its ability to surprise the enemy to great effect. A controversial text authored by two then- PLA colonels underscores the potential of cyber-attacks against the financial institutions of superior states,[10] particularly as a first strike option. According to James Mulvenon, a noted Chinese information warfare expert, "PLA writings generally hold that information warfare is an unconventional warfare weapon, not a battlefield force multiplier... that will permit China to fight and win an information campaign, precluding the need for military action."[11]

While information war encompasses a broader space of engagement, cyberspace is but one part of the larger information domain. Information

space refers to "the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself."[12] Per China's perspective, the main function of the information space is "for people to acquire and process data... a new place to communicate with people and activities, it is the integration of all the world's communications networks, databases, and information, forming a landscape."[13] As such, China sees a larger threat space extending beyond the digital confines of the Internet.

Russian Writing on Information Warfare

Like China, Russia refers to "information space" as a holistic term. In 2010, the Russian government updated its Military Doctrine in which "cyber warfare" was notably omitted (like the Chinese, the Russians use the term "information" rather than the more popularized term "cyber"). However, there were several references to "information warfare" that by definition would include offensive attacks against information systems (i.e., computers) and/or the information resident on them. More importantly, the doctrine recognized the information space as a critical area that the military must protect from outside threats. This bolsters dictums in Russia's 2000 Information Security Doctrine, in which the protection against foreign harmful information and the promotion of patriotic values were identified as national security objectives.[14] Other objectives cited in the 2010 *Military Doctrine* include:[15]

> ...developing goals and resources for information warfare..... to create new models of high-precision weapons and develop information support for them...prior implementation of measures of informational warfare in order to achieve political objectives without the utilization of military forces.

Russian information warfare theory is rooted in the idea that Russia must "respond with war to the information war waged against Russia,"[16]and covers a broad range of actions including political, economic, cultural, and military, to name a few. Russian authors understand information warfare as influencing the consciousness of the masses as part of the rivalry between the different civilian national systems adopted by different countries in the information space. These are put into effect by use of special means to control information sources as "information weapons."[17] Russia defines

"information space" as "the sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and the information itself."[18] As such, it is the technical (e.g., the physical destruction of an information system a la Stuxnet) and psychological (e.g., influencing and manipulating a population) effect of that space that worries Russia.

Consistent with this broad interpretation of the information space, Russia cites "information weapons" as weapons of concern. By their very definition, information weapons can be used in domains other than cyber, including the human cognitive domain,[19] and include geographic areas where the Russian language is used and a Russian diaspora exists.[20] Certainly Russia viewed the successes of the "Color Revolutions" and the "Arab Spring" as examples of failed information and social control.

U.S. Writing on Information Warfare

The U.S. views cyberspace as the networks and systems that comprise its architecture, rather than the entire information environment akin to the Chinese/Russian definition of information space. The U.S. has published numerous strategic and operational pieces providing insight into how the military should operate in the cyber domain via information operations (IO), of which cyber operations (aka "cyber warfare") is but one of several components. The 2011 Department of Defense's Strategy for Operating in Cyberspace as well as the 2012 revision of its Joint Publication on Information Operations (JP 3-13) reflects recent U.S. military thinking on cyberspace as a warfare arena. Indeed, the establishment of U.S. Cyber Command (CYBERCOM) is in line with the U.S. commitment to operating freely in cyberspace while hindering the adversary's capabilities. According to the Strategy document, CYBERCOM reflects the following goals:

> To ensure the development of integrated capabilities by working closely with Combatant Commands, Services, Agencies, and the acquisition community to rapidly deliver and deploy innovative capabilities where they are needed the most.[21]

The JP 3-13 provides information as to the deployment of cyber capabilities. It sets forth doctrine and guidance governing the activities of the U.S. military in joint operations. According to JP-313:

> Information operations (which include computer network operations) are designed to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.[22]

The key difference between the writings of China/ Russia and the U.S. lies in a holistic interpretation versus a more narrowed perspective of the threat space. China/ Russia prefer to combine the human and technological aspects, while the U.S. focuses solely on the technological aspects. The U.S. views a larger IO campaign as consisting of several separate, albeit possibly interrelated, military capabilities, whereas China/ Russia emphasize a more interconnected perspective where there is no clear separation between the activities conducted or the effects achieved. In this context, a cyber-attack can consist of malware deployment against a critical infrastructure (per the U.S. perception), or hostile information directed against the government or its populace by adversarial oppositionist forces (per the China/Russia perceptions).

Cyber-Attack Incidents

Several high profile cyber-attacks reveal an evolution from disruptive to destructive force. This is not to say that all future cyber-attacks will involve the destruction of information systems, only that in certain instances where opposing factions are entrenched in diplomatic confrontation, precedent has been established where destruction may be a viable option. In the incidents highlighted below, nation state direction or sponsorship was largely suspected but never proven, suggesting that if governments were involved in orchestrating attacks, they preferred to use them as surprise weapons during times of diplomatic tension, with plausible deniability, and in engagements with limited or non-existent force-on-force operations.

2013 South Korea Wiper Malware

In March 2013, "wiper malware" deleted data on three South Korean banks' systems and their insurance affiliates, as well as three broadcasting organizations. While the majority of the attacks occurred on March 20, evidence suggested that in some cases systems have been previously infected with malware set to deploy on that date.[23] The malware overwrote the Master Boot Record of the computers running these networks, as well as disabling

the antivirus program from a well-known South Korean company.[24] The attack was estimated to have compromised 48,000 computers.[25]

This event marked the fourth in a series of well publicized attacks employing wiper malware, the first being the April 2012 wiper malware against Iran's Khang Island facility, the second being the Saudi Aramco incident, and the third being the Qatari RasGas incident. Notably, this indicates a shift toward more destructive attacks by non-state actors during times of political tension. Like the Aramco incident, a previously unknown group ("WHOIS") claimed responsibility,[26] though the reliability of this attribution was called into question due to the questionable history and demonstrated capability to execute this level of attack.

South Korean officials believed North Korea military intelligence units were responsible, operating from Chinese IP addresses.[27] In the frameworks of the prolonged north-south conflict, political and diplomatic rhetoric has often spilled into the cyber domain at least since 2009 when botnets directed DDoS attacks against South Korean and U.S. websites.[28] Prior to March 2013, North Korea ramped up its threats against South Korea and the U.S. during the March 11-21 joint Key Resolve military exercises (which occurred right after the North Korean testing of its nuclear device in February 2013).[29] If North Korea was behind the attacks, they represented a divergence from a usually robust albeit benign DDoS activity. More importantly, the incident signaled to Seoul that the North was capable of conducting destructive cyber-attacks if it perceived transgressions against established "norms" between the two governments.

2012 Saudi Aramco Wiper Malware

In August 2012, a virus erased data on three-quarters of the corporate computers of Saudi Aramco, Saudi Arabia's national oil company, largely considered the world's most valuable company.[30] The malware was designed to accomplish two objectives: 1) replace the data on hard drives with an image of a burning American flag and report a list of infected addresses back to a computer inside the company's network, and 2) wipe the memories of the infected computers.[31] Labeled "Shamoon," the virus destroyed the hard drives on 30,000 computers.[32]

The event's significance lay in the fact that malware was purposefully deployed to destroy as many computer hard drives as possible in a company involved in critical infrastructure. The malware's sophistication is debatable; then-U.S. Defense Secretary Leon Panetta referred to the Shamoon virus

as a very sophisticated tool,[33] while other security researchers from Kaspersky Lab suggested that coding errors in the code were indicative of amateurish work and the malware could have been more destructive.[34] The virus was released against Aramco the day before one of the holiest nights of the Islamic year.[35] This suggests that the attackers wanted to enhance operational success, correctly estimating that there would be limited monitoring during this period, allowing time for the virus to deploy and spread. The attack impacted oil production as well as business practices of the company as some drilling and production data was probably lost.[36] According to one source, it took ten days to replace infected hard drives.[37]

Though a previously unknown activist group called "The Cutting Sword of Justice" claimed responsibility for the attack, stating that it was a response to Saudi policies in the Middle East,[38] many people including unnamed U.S. government officials suspected Iranian involvement.[39] If Tehran was the orchestrator, it preferred to engage Saudi Arabia covertly using a proxy in order to maintain plausible deniability, particularly as the attack directly targeted a major global oil producer and critical infrastructure. While there has been no international consensus as to what constitutes a "red line" in cyberspace, it would stand to reason that the purposeful destruction affecting a global enterprise would be considered an act of force as defined by the International Humanitarian Law of Armed Conflict, which regulates the conduct of armed hostilities between nation states. In this context, the targeting of Saudi Aramco – a symbol of Saudi power – could be interpreted as an Iranian signal to Riyadh of its discontent regarding Aramco benefits from U.N.-imposed sanctions on Iran, as well as Riyadh's perceived collaboration with the U.S. over Iran's nuclear aspirations.

2010 Stuxnet Attack on Iranian Centrifuges

Stuxnet is believed to be closely related to three other equally, if not more sophisticated, malware items known as Duqu, Flame, and Gauss. Since their purposes are more consistent with cyber espionage, they are not included in the current paper.

In 2010, Tehran disclosed that a cyber-weapon, coined "Stuxnet" by a Microsoft researcher, had damaged gas centrifuges in an Iranian uranium enrichment facility. Stuxnet was described as a "highly sophisticated" and complex application designed for the sole purpose of sabotaging uranium enrichment centrifuges controlled by high-frequency converter drivers used by the uranium enrichment facility at Natanz.[40] Approximately 1,000

centrifuges were impacted by the malware, causing them to spin out of control and ultimately require replacement.[41]

Stuxnet was significant in that it was the first incident of a cyber-weapon created and deployed with the intent of degrading, disrupting, and destroying a specific information system. Perhaps more importantly, the malware's sophistication, as well as its clandestine appearance on an industrial control system network air-gapped from the Internet in a secured environment pointed directly at nation state sponsorship. Despite being discovered in 2010, Stuxnet is believed to have been deployed as early as 2009,[42] indicating that a surreptitious delivery against this target was a successful approach. No other group assumed responsibility.

Iran had made it clear on several occasions that it intended to exercise its sovereign right to develop its nuclear program for peaceful purposes,[43] causing great concern for the U.S., as well as other Western and Middle Eastern states, and even Iran-friendly China and Russia.[44] While Stuxnet remains officially unattributed to any government, it is widely suspected to be the result of a U.S./Israel partnership.[45] The successful deployment negated the need for a conventional military strike that risked escalatory retaliation. If the U.S. was behind Stuxnet, the incident could be interpreted as a U.S. signal to Iran that Washington remained committed to not allowing Iran to enrich uranium for weapons purposes, demonstrating that it was able to reach out and gain access to a sensitive and well protected facility with a weapon of destruction.[46]

2008 Georgia DDoS Attacks

In August 2008, Russian forces invaded Georgia as a result of Tbilisi's decision to launch a surprise attack against separatist forces in South Ossetia.[47] Prior to the Russian counter invasion, cyber-attacks were already being launched against Georgian governmental websites.[48] Lasting for most of August, these digital attacks consisted mostly of website defacements (particularly against government websites) and DDoS attacks that targeted media sites, financial institutions, a Georgian hacker community site, and Georgian government sites.[49]

The cyber-attacks were notable for one main reason: they coincided with the Russian military invasion. In many ways, the 2008 cyber-attacks were very similar to the 2007 attacks: defacements and DDoS targeted the private and public sectors. The uniqueness of these attacks lay in their coordination and intensity, as opposed to gradual coordination as was the

case in Estonia.[50] If the same actors or types of actors were involved, they made adjustments to their attack methodology for maximum effectiveness.

Like in Estonia, the attacks were attributed to Russian nationalistic hackers, with Moscow suspected as being their sponsor.[51] If Moscow was again the orchestrator, these attacks could be interpreted as a "lessons learned" exercise in targeting a country via cyber weapons. While infrastructure was the main target in Estonia, media and news organizations were the prime victims in Georgia. By targeting these outlets, the attackers sought to control Georgia's information space and prevent anti-Russian sentiment from being broadcast, a Russian information warfare concept conveyed by leading Russian information warfare theorists such as Igor Panarin.[52] Ultimately, however, these efforts to control information failed, with many believing that Georgia won the information war.[53] Nevertheless, this incident demonstrated that even during force-on-force engagement, Moscow preferred to maintain plausible deniability. One would think that once physical strikes were conducted, the need to conceal cyber operations – particularly if they were not seeking to destroy information systems or the information resident on them – would be moot, especially when considering a nation state that is equal to the U.S. in cyber capability.[54] Nevertheless, the Georgian DDoS attacks signaled to Russia's neighbors and former states that they may be targeted by the same type of activity should their governments enter heightened periods of diplomatic tension with the Russian Federation.

Actual Military Conflict

Not all military-on-military or force-on-force engagements featured cyber-attacks as a primary or supporting military component. This bears noting given that some of the countries involved are capable actors known to have formalized doctrinal writings on how cyber-attacks could and should be used in conflict scenarios. While the absence of strategic cyber-attacks could be interpreted as a lack of viable strategic cyber targets, evidence suggests they were not employed largely because no strategic advantage would be gained, thereby calling into question the efficacy of cyber-attacks as viable weapons to achieve similar results as conventional weapons.

2014 Israel-Hamas Crisis

In July 2014, Israel launched a missile at Gaza's only electricity plant causing the termination of all electricity in the area, which would worsen existing

problems with water and sewage, according to press reports.[55] The use of conventional weapons against this target could have been prompted by Israel's inability to successfully target the plant via cyber means. However, this seems implausible based on Israel's reputation as a leading cyber power and its suspected involvement in some well publicized cyber incidents such as the 2012 cyber-attacks targeting a power plant and other Iranian industries,[56] the 2010 Stuxnet attacks against Iranian nuclear centrifuges,[57] and the 2007 cyber-attacks against Syrian air defense systems.[58] In order to achieve the strategic objective of disabling a key target, it can be inferred that the implementation of kinetic weapons was preferred as a more reliable course of action to support the immediate objectives of the mission.

2014 Ukraine-Russia Crisis

During the 2014 Ukraine-Russia crisis, the Ukrainian telecommunications company Ukrtelecom reported that armed men raided its facilities in Crimea on February 28 and tampered with fiber optic cables, causing outages of local telephone and Internet systems.[59] Given assessments of Russia's proficiency in cyber operations,[60] as well as the fact that much of Ukrainian telecommunications was built when it was part of the Soviet Union, one would think that a cyber-attack would be a feasible course of action given knowledge of the target and the benefits of disrupting cyberspace. Previous Russian nationalist hacker activity (e.g., 2007 Estonia and 2008 Georgia) would further suggest that such an action could have been viable, if not preferential. However, cyber-attacks against the Ukraine did not ensue. Furthermore, while open source reports referenced "cyber skirmishes" transpiring between pro-separatist and pro-Ukraine interests, as of June 2014 there was no evidence of significant activity impacting key critical infrastructure or command-and-control targets.

2013 Syrian Civil War

According to a 2014 *New York Times* article, when Syria experienced an uprising against its government, the Pentagon and the National Security Agency developed a battle plan that featured a sophisticated cyber-attack on the Syrian military and President Bashar al-Assad's command structure.[61] However, according to the same article, President Obama turned it down (as well as other conventional strike options) based on the limited strategic value of the mission, coupled with the untested ability of cyber weapons during a military conflict.[62] The Obama administration remained unsure

whether cyber weapons were a useful military tool, or if they should be reserved for covert operations.[63]

2011 Libyan Civil War

In 2011, the U.S. considered deploying cyber weapons against Libya. According to open source reports, the goal would have been to break through the Libyan government's firewalls to sever military communications links and prevent early-warning radars from gathering information and relaying it to missile batteries aimed at NATO warplanes.[64] However, once the U.S. militarily committed to the use of force, the U.S. relied on conventional weapons to accomplish the same task. While there has been some debate as to the reason behind this (two popular beliefs are that the U.S. did not want to show its capabilities, and it did not want to be the first to use cyber-weapons in this manner),[65] perhaps a more pressing concern was whether or not cyber-attacks could have achieved the same level of military effectiveness as conventional missile strikes.

Conclusion

There is little doubt that foreign governments are developing cyber capabilities, whether to bolster their respective intelligence collection apparatuses or as instruments of nation state power. The military and academic writings of three prominent nation states advocate the use of cyber weapons, particularly against critical infrastructures, in time of state conflict. History is ripe with incidents in which a military targeted an adversary's critical infrastructures during wartime for both tactical and strategic advantage. Therefore, it follows that computer-based weapons could be leveraged in a similar manner.

Nevertheless, most of the observed cyber activities executed against state targets have come during times of diplomatic tension and conducted largely by non-state actors operating as state proxies. Cyber-attacks have been most effective as first-strike weapons benefiting from surprise and the anonymity afforded to them by the difficulties of attribution. In conflicts where military forces were involved (and therefore the need for non-attribution is less important), there were limited instances where cyber-attacks were implemented as either a decisive or supporting component to achieving a military objective. In most cases, physical strikes were the chosen course of action, perhaps as a more reliable and expedient alternative.

In the immediate future, it appears that cyber weapons are better built for surreptitious activity and state signaling rather than as imposing wartime game-changers. That is not to say this will not change in time, but it is going to require nation states to actually use them during conflict, experience the problems that occur during their deployment, and apply lessons-learned to improve their effectiveness. Thus far, this has not been done begging the question: do cyber weapons have a role in conflict? As militaries include technology into their operations, the answer is "yes" – just not a resounding one.

Notes

1 Thomas Rid and Peter McBurney, "Cyber Weapons," *Rusi Journal*, February/March 2012, https://www.rusi.org/downloads/assets/201202_Rid_and_McBurney.pdf.

2 Department of Homeland Security, "What is Critical Infrastructure?" November 1, 2013, http://www.dhs.gov/what-critical-infrastructure.

3 Daniel T. Kuehl, "Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age," *International Law Studies* 76 (2002).

4 "DoD Directive TS3600.1," *IT Law Wiki*, http://itlaw.wikia.com/wiki/DOD_Directive_TS3600.1.

5 Michael Breen and Johsua A. Geltzer, "Asymmetric Strategies as Strategies of the Strong," *Parameters* (Spring 2001), http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2011spring/Breen-Geltzer.pdf.

6 Shen Weiguang, "Focus of Contemporary World Military Revolution—Introduction to Information Warfare," *Jiefangjun Bao* (November 7, 1995): 6.

7 Major General Wang PuFeng, *The Challenge of Information Warfare* (1995), http://fas.org/irp/world/china/docs/iw_mg_wang.htm.

8 Liu Yichang, ed., *Gaojishu Zhanzheng lun* (On High-Tech War) (Beijing: Military Sciences Publishing House, 1993), p. 272.

9 Deepak Sharma, "Integrated Network Electronic Warfare: China's New Concept on Information Warfare," *Journal of Defense Studies* 4, no. 2 (April 2010).

10 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), p. 168.

11 James C. Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, Mulvenon and Yang, eds. (Washington DC: RAND, 1999), pp.175-86.

12 Keir Giles and William Hagestad, "Divided by a Common Language: Cyber Definitions in Chinese, Russian, and English," 2013 5th International Conference on Cyber Conflict, (NATO: CCD COE Publications).

13 Ibid.

14 Doctrine of Information Security of the Russian Federation. (2000). Taken from http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument.
15 Russian Military Doctrine (2010). Taken from http://carnegieendowment.org/files/2010russia_military_doctrine.pdf
16 Jolanta Darczewska, "The Anatomy of Russian Information Warfare," *Point of View* 42 (May 2014), http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.
17 Ibid.
18 Giles and Hagestad, "Divided by a Common Language."
19 Ibid.
20 Darczewska, "The Anatomy of Russian Information Warfare."
21 Department of Defense "Department of Defense's Strategy for Operating in Cyberspace – July 2011," http://www.defense.gov/news/d20110714cyber.pdf.
22 Joint Publications 3-13 Information Operations," Department of Defense, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.
23 Matthew J. Schwartz, "North Korea Behind Bank Malware, South Korea Says," *Dark Reading (*April 10, 2013), http://www.darkreading.com/attacks-and-breaches/north-korea-behind-bank-malware-south-korea-says/d/d-id/1109474?.
24 Michael Mimoso, "Theories Abound on Wiper Malware Attack against South Korea," ThreatPost (March 21, 2013), http://threatpost.com/theories-abound-wiper-malware-attack-against-south-korea-032113/77654.
25 Schwartz, "North Korea Behind Bank Malware."
26 "Wiper Malware Analysis Attacking Korean Financial Sector," Dell Secure Works (March 21, 2013), http://www.secureworks.com/cyber-threat-intelligence/threats/wiper-malware-analysis-attacking-korean-financial-sector/.
27 Sean Gallagher, "North Korean Military Blamed for Wiper Cyber-Attacks against South Korea," ArsTechnica (April 10, 2013), http://arstechnica.com/security/2013/04/north-korean-military-blamed-for-wiper-cyber-attacks/.
28 Choe Sang-Hun and John Markoff, "Cyber-Attacks Jam Government and Commercial Websites in U.S. and South Korea," *New York Times* (July 8, 2009), http://www.nytimes.com/2009/07/09/technology/09cyber.html.
29 Comprehensive Nuclear Test Ban Treaty Organization, "On the CBTO's Detection in North Korea," February 12, 2013, http://www.ctbto.org/press-centre/press-releases/2013/on-the-ctbtos-detection-in-north-korea/.
30 Nicole Perlroth, "In Cyberattack on Saudi Firm, U.S Sees Iran Firing Back," *New York Times* (October 23, 2012), http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all.
31 Ibid.

32 Kelly Jackson Higgins, "The Long Shadow of Saudi Aramco," *Dark Reading*, October 14, 2013, http://www.darkreading.com/attacks-breaches/the-long-shadow-of-saudi-aramco/d/d-id/1140664?.

33 Phil Stewart, "Shamoon Virus Most Destructive Yet for Private Sector, Panetta Says," *Reuters* (October 11, 2012), http://www.reuters.com/article/2012/10/12/us-usa-cyber-pentagon-shimoon-idUSBRE89B04Y20121012.

34 Fahmida Y. Rashid, "Coding Errors in Shamoon Malware Suggest It May Be the Work of Amateurs," *Security Week*, September 12, 2012, http://www.securityweek.com/coding-errors-shamoon-malware-suggest-it-may-be-work-amateurs.

35 Paul Roberts, "Whoddunnit? Conflicting Accounts on Aramco Hack Underscores Difficulty of Attribution," Naked Security, October 30, 2012, http://nakedsecurity.sophos.com/2012/10/30/whodunnit-aramco-hack/.

36 John Roberts, "Cyber Threats to Energy Security as Experienced by Saudi Arabia," Platts, November 27, 2012, http://blogs.platts.com/2012/11/27/virus_threats/#comments.

37 Roberts, "Whoddunnit?"

38 Perlroth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back."

39 Siobhan Gorman and Julian E. Barnes, "Iran Blamed for Cyber Attacks," *Wall Street Journal*, October 12, 2012, http://online.wsj.com/news/articles/SB10000872396390444657804578052931555576700.

40 Matthew Schwartz, "Stuxnet Launched by United States and Israel," *Information Week*, June 1, 2012, http://www.reuters.com/article/2011/12/02/us-cyberattack-iran-idUSTRE7B10AV20111202.

41 Ellen Nakashima, Greg Miller, and Julie Tate, "U.S. Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," *Washington Post*, June 19, 2012, http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

42 "Stuxnet Effect: Iran Still Reeling," Industrial Safety and Security Source, August 3, 2011, http://www.isssource.com/stuxnet-affect-iran-still-reeling/.

43 "Timeline of Iran's Controversial Nuclear Program," *CNN*, March 19, 2012, http://www.cnn.com/2012/03/06/world/meast/iran-timeline/.

44 Max Fisher, "Nine Questions about Iran's Nuclear Program You Were Afraid to Ask," *Washington Post*, May 19, 2013, http://www.washingtonpost.com/blogs/worldviews/wp/2013/11/25/9-questions-about-irans-nuclear-program-you-were-too-embarrassed-to-ask/.

45 David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0.

46 Emilio Iasiello, "Cyber-Attack: A Dull Tool to Sharpen Foreign Policy," 2013 5th International Conference of Cyber Conflict, 2013, http://www.ccdcoe.org/publications/2013proceedings/d3r1s3_Iasiello.pdf.

47 Council of Europe Parliamentary Assembly Resolution 1633 (2008) on "The Consequences of War Between Georgia and the Russian Federation," available at http://assembly.coe.int/ASP/Doc/XrefViewHTML.asp?FileID=12031&Language=en.

48 EnekenTikk, KadriKaska, and LiisVihul, "International Cyber Incidents: Legal Considerations," Cooperative Cyber Defense Center of Excellence, 2010, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

49 Ibid.

50 Eneken, Kadri and Liis "International Cyber Incidents."

51 Ibid.

52 Darczewska, "The Anatomy of Russian Information Warfare."

53 Clifford J. Levy, "Russia Prevailed on the Ground but not in the Media," *New York Times*, August 21, 2008, http://www.nytimes.com/2008/08/22/world/europe/22moscow.html?_r=0.

54 Keir Giles, "Information Troops – a Russian Cyber Command?" 2011 3rd International Conference on Cyber Conflict (CCD COE Publications: 2011), http://www.ccdcoe.org/publications/2011proceedings/InformationTroopsARussianCyberCommand-Giles.pdf

55 Alan Greenblatt, "Israeli Bombing Ruins Gaza's only Power Plant," *NPR*, July 29, 2014, http://www.npr.org/blogs/thetwo-way/2014/07/29/336386340/israeli-bombing-destroys-gazas-only-power-plant.

56 Rick Gladstone, "Iran Blames US and Israel for Spree of Cyber Attacks," *Sydney Morning Herald*, December 27, 2012, http://www.smh.com.au/it-pro/security-it/iran-blames-us-and-israel-for-spree-of-cyber-attacks-20121226-2bwa1.html.

57 Ellen Nakashima and John Warrick, "Stuxnet Was Work of US and Israel, Experts Say," *Washington Post*, June 2, 2012, http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

58 John Leyden, "Israel Suspected of Hacking Syrian Air Defenses," *The Register*, October 4, 2007, http://www.theregister.co.uk/2007/10/04/radar_hack_raid/.

59 Polityuk, P. and Finkle, J. "Ukraine Says Communications Hit, MPs Phones Blocked." *Reuters,* April 3, 2014, Taken from http://www.reuters.com/article/2014/03/04/us-ukraine-crisis-cybersecurity-idUSBREA231R220140304.

60 Smith, D., *Russia Cyberoperations* (Washington, D.C.: Potomac Institute Cyber Center, 2010), http://www.potomacinstitute.org/attachments/article/1273/Russian%20Cyber%20Operations.pdf.

61 David E. Sanger, "Syria Stirs New U.S. Debate on Cyberattacks," *New York Times*, February 25, 2014, http://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html.

62 Ibid.

63 Ibid.

64 Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *New York Times*, October 17, 2011, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

65 Jack Goldsmith, "Quick Thoughts on the USG's Refusal to Use Cyberattacks in Libya," Lawfare Blog, October 18, 2011, http://www.lawfareblog.com/2011/10/quick-thoughts-on-the-aborted-u-s-cyberattacks-on-libya/.