SMALL WARS JOURNAL

Terrorism, War, and Cyber (In)Security

By ***José de Arimatéia da Cruz***
Journal Article | *Oct 27 2013 - 4:17pm*

Terrorism, War, and Cyber (In)Security

José de Arimatéia da Cruz

Introduction

> "*The supreme art of war is to subdue the enemy without fighting*"
>
> -Sun Tzu's *The Art of War*

It has become a cliché to state that in the twenty-first century we live in post-industrial and globalized world. The terms post-industrial world and globalized world are used interchangeably to mean that we live in a society that competes within a world economy, most of its citizens are employed within the service sector, and society dominates the production and manipulation of information technology, that is, computer technology.

One of the consequences for the nation-state in a global interconnected society is that its critical infrastructures (CIs) composed of public and private institutions of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials sectors become vulnerable to cyber-terrorism. Audrey Kurth Cronin pointed out, "insurgents and terrorist groups have effectively used the Internet to support their operations for at least a decade. The tools of the global information age have helped them with administrative tasks, coordination of operations, recruitment of potential members, and communications among adherents" (Cronin, 2013).

In the traditional view of political realism, the nation-state is the primary unit of analysis and a sovereign hegemon. However, in the cyber world of the twenty-first century, the Internet is seen as the realization of the classic international relations theory of an anarchic, leaderless world (Schmidt and Cohen, 2013). In the anarchical international system of the twenty-first century, each nation-state must protect its geographical borders against both domestic and foreign enemies, although from a realist perspective greater emphasis is given to external threats at the expense of domestic protection. The enemy is always a sovereign nation with geographical boundaries, a population, and usually a legitimate or recognizable government. The *raison d'etat* is to protect or ensure the security of the homeland first and foremost against an enemy attack, either domestic or foreign. The traditional notion of national security from a realist perspective is not only obsolete but also does not recognize the security complexities of the twenty-first century in the information age. "Being by far the strongest actor in the international system,"

according to Audrey Kurth Cronin, "the state is quickly catching up and learning to more effectively monitor, consider, and employ these technological means of mobilization, both defensively and offensively; however, some states are harnessing and exploiting them more quickly than others and, for good or for ill, gaining relative advantage for their own ends" (Cronin, 2013). Clay Wilson corroborates Cronin's argument in that "terrorist groups, through use of the Internet, are now challenging the monopoly over mass communications that both state-owned and commercial media have long exercised. A strategy of the terrorists is to propagate their messages quickly and repeat them until they have saturated cyberspace. Internet messages by terrorist groups have become increasingly sophisticated through the use of a cadre of Internet specialists who operate computer servers worldwide" (Wilson, 2007).

The argument put forward here is based on the transformation thesis which argues that cyber terrorism is "criminal or harmful activities that are informational, global, and networked". They are the product of networked technologies that have transformed the division of criminal labor to provide entirely new opportunities for, and indeed, new forms of crime which typically involves the acquisition or manipulation of information and its value across global networks" (Wall, 2008). In the post-industrial, globalized, and media-centric society of the twenty-first century, the Internet "is seen as a part of the globalization process that is sweeping away old realities and certainties, creating new opportunities and challenges associated with living in a shrinking world" (Yar, 2006). Information operations (IOs) traditionally associated with the military establishment and one of the tools in the arsenal of military planners is no longer just limited to the armed forces. The Department of Defense (DoD) defines information operations as actions taken during a time of crisis or conflict to effect the adversary's information, while defending one's own information systems, to achieve or promote specific objectives (DoD, 2003).

Terrorist organizations are also utilizing the Internet as an essential part of its information operations (IOs) offensive strategic objectives as future conflicts in the twenty-first century will extend into the cyberspace domain from the physical domain. President Obama in his "International Strategy for Cyberspace," acknowledged that, "cybersecurity threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace" (International Strategy for Cyberspace, 2011).

Why Cyber-terror?

Nation-states as well as individuals depend on the Internet on a daily basis to conduct business, schedule a vacation, purchase goods and services, trade, connect with long lost friends, and even find love. To argue that the Internet has become an integral part of our coexistence in this planet is no exaggeration. Recep Tayyip Erdogan, Turkey's Prime Minister, on June 2, 2013, argued that, "social media are the worst menace to society" (*The Economist*, 2013). President Barack Obama has described the Internet as "the backbone that underpins a prosperous economy and a strong military and an open and efficient government" (Obama, 2009). At his confirmation hearing, Secretary of State John Kerry called cyber-attacks against the U.S.'s critical infrastructure a "twenty-first century nuclear weapons equivalent" (Negroponte and Palmisano, 2013).

The Internet allows individuals from different quarters of the globe to communicate instantaneously by sending and receiving e-mails, using Face Time, or using Internet Relay Chat (IRC). These communications take place between users and web pages thus creating what Jack Goldsmith and Tim Wu, in their book *Who Controls the Internet? Illusions of a Borderless World*, call the "death of distance" (Goldsmith and Wu, 2006). Goldsmith and Wu argue that the Internet traffic appears to decline with distance and is increasingly concentrated within localities, countries, and regions (Goldsmith and Wu, 2006). The implosion of the Soviet Union and the end of the Cold War may not have led to the end of the history as proclaimed by Francis Fukuyama in his seminal work *End of History and the Last Man*; but,

instead, the social, economic, and political transformations taking place with the advancement of the Internet in the last two decades has led to the "end of geography," where geographic borders between countries becomes more porous with the advancement of the informational society.

The Internet transcends international boundaries, ignores ethnic divides, and remains relatively unyielding to the efforts of security and security forces ("Theater of Jihad," 2009). Unlike traditional crime scenes, the Internet does not leave a fingerprint and prosecution is hardly ever accomplished given the Internet's attribution problem. An attacked nation(s) may know where an attack is coming from but they can not be certain of the source or who is behind it since terrorist organizations usually prefer to seize control of intermediary systems to do their work ~~so~~ to prevent tracing. One of the favorite cyber techniques used by cyber-terrorists and jihadists is a technique known as the "man-in-the-middle" attack. As Eric Schmidt and Jared Cohen explains in their book *The New Digital Age: Reshaping the Future of Peoples, Nations and Business (2013)* the "man-in-the-middle" is an attack where "a third party attacker inserts himself between two participants in a conversation and automatically relays messages between them, without either participants realizing it. This third party acts like an invisible intermediary, having tricked each participant into believing that the attacker is actually the other party of the conversation" (Schmidt and Cohen, 2013).

The attribution problem is further complicated due to four additional factors. First, cyber attacks do not require geographic proximity to a desired target. Second, there is no equivalent to radar systems to detect the origin of an attack. Third, the protocols that govern Internet traffic are insecure and the origin of packets can be masked. Fourth, cyber attacks will typically use one or more compromised systems as the launching point for their attack, crossing multiple international boundaries in order to complicate the investigation process (Knake, 2010). According to Debra Littlejohn Shinder, a technology consultant, "cybertorrists can use standard malware distribution techniques to install remote control software on computers and turn them into zombies that are part of a huge botnet. The botmaster can then use these computers to launch Distributed Denial of Service (DDoS) attacks against those critical targets" (Shinder, 2011). As a result, geographical boundaries become irrelevant in preventing terrorist organizations worldwide from carrying out cyber attacks. The proliferation of new technologies in the twenty-first century allows individual's "frustrations to be rapidly shaped, exploited, formed, and mobilized into violent expression by territorially disjointed groups who are then able to act together" (Cronin, 2013).

The term cyber terrorism means the "exploitation of electronic vulnerabilities by terrorist groups in pursuit of their political aims" (Yar, 2006). This definition is just one of many definitions since there is no consensus among scholars in the cybersecurity literature on an operational definition of cyber terrorism. For example, Verton (2003) defines cyber terrorism as the use of "execution of a surprise attack by a sub-national foreign terrorist group or individuals with a domestic political agenda using computer technology and the Internet to cripple or disable a nation's electronic and physical infrastructures." Dorothy E. Denning, a professor in the Department of Defense Analysis at the Naval Postgraduate School, (2000) defines the term cyber terrorism with several qualifications to denote the:

> Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructure could be acts of cyber terrorism, depending on their impact. Attacks that

> disrupt nonessential services or that are mainly a costly nuisance would not.

In spite of a lack of an operational definition, cyber terrorism is real and it has become the new tool of terrorists, jihadists, and transnational criminal organizations (TCOs) worldwide. James Clapper, U.S. Director of National Intelligence, for the first time declared that cyber-threats represent the greatest danger facing the nation, bumping terrorism down to second place (Bamford, 2013). During his testimony regarding the 2007 Annual Threat Assessment, former FBI Director Robert Mueller stated that, "terrorists increasingly use the Internet to communicate, conduct operational planning, proselytize, recruit, train and to obtain logistical and financial support. That is a growing and increasing concern for us" (Mueller, 2007). For example, Hezbollah, the Lebanese-based Shiite Islamic group also known as Islamic Jihad, established its collection of web sites in 1995. The Hamas, the Palestinian militant Islamic fundamentalist group presents political cartoons, streaming video clips, and photomontages depicting the violent deaths of Palestinian children by Israeli soldiers. The Liberation Tigers of Tamil Eelam (LTTE), a guerrilla force in Sri Lanka offers daily position papers, daily news, and an online store –for sale are books, pamphlets, videos, audiotapes, and CDs. The State University of New York at Binghamton hosted the website of the Revolutionary Armed Forces of Colombia (FARC) while the University of California in San Diego hosted the website for the Peruvian guerrilla group Tupac Amaru (MRTA) (Conway, 2002).

Terrorists and jihadist organizations have recognized the importance of the Internet as part of their arsenal of weapons in the "theater of fear" as they attempt to win the hearts and minds of perspective sympathizers and recruits. The Internet has become one of the most important tools in al-Qaeda's war against the infidels and their supporters. So-called jihadist websites have proliferated in the aftermath of September the 11th terrorist attacks against the U.S. Not only has there been a proliferation of jihadist websites but the quality, contents, and messages have also become more sophisticated and professional. The Quetta Shura Taliban maintains several dedicated websites, including one with an Arabic-language online magazine and daily electronic press releases on other Arabic-language jihadist forums. The As-Shabab Institute for Media Production is al-Qaeda Central's media arm distributing video, audio, and graphics products online through jihadist forums, blogs, and file-hosting websites (Theohary and Rollins, 2011). During counterterrorism operations in Iraq a letter dated July 9, 2005 from Ayman al-Zawahiri to Abu Musab al-Zarqawi was obtained. In that letter, al-Zawahiri acknowledged the importance of the Internet and he wrote, "we are in a battle, and more than half of this battle is taking place in the battlefield of the media" (al-Zawahiri, 2005).

Why cyber terror when perhaps a physical attack would cause more damage and bring greater worldwide publicity? The transition from terrestrial to virtual attacks, according to Yar (2006), is deemed to offer a number of advantages to terrorist groups. First, the Internet, by its nature, enables "action from a distance." Terrorists no longer need to gain physical access to a particular location since the proliferation of Internet café's worldwide can provide terrorist organizations as well as transnational criminal organizations with electronic access to any system from anywhere in the world. Furthermore, by staging cyber-attacks from within the borders of so-called "rogue states" or "failed states," it is possible to exploit a "safe haven" lying outside the reach of security and criminal justice agencies in the target nations. The Independent Task Force Report No. 70 by the Council on Foreign Relations suggests that "government authorities need to work across borders to fight crime and prevent terrorist attacks. But, many lawful intercept regulations—demands for communications network data for the purpose of analysis or evidence—are inconsistent and often burdensome to business and overly broad, threatening user privacy" (Negroponte and Palmisano, 2013).

Second, the Internet turns actors with relatively small numbers and limited financial and material

resources into what has been dubbed “the empowered small agents.” This empowerment effect stems from the Internet’s ability to become a “force multiplier,” that is, something that can “increase the striking potential of a unit without increasing its personnel” (White, 1991).

Third, cyber-terrorism also allows terrorist organizations a certain degree of anonymity. Flemming and Stohl (2000) have argued that one of the greatest challenges to government agencies is the extent to which the Internet environment affords perpetrators the ability to disguise itself. Furthermore, according to Denning (1999), total anonymity affords the criminal the ability to launder money and engage in other illicit activities in ways that circumvent law enforcement. Combined with encryption or steganography and anonymous re-mailers, digital cash could be used to traffic in stolen intellectual property on the Web or to extort money from victims.

Steganography dates back to ancient Greece when the Greek historian Herodotus explained how his fellow countrymen would send secret messages back and forth, warning of potential invasion. The Greeks had discovered that if you melted wax off a table, scratched the message on the wood underneath, and reapplied a fresh layer of wax, the message would be hidden and secret (Rogers, 2005). The term steganography comes from the Greek word *steganos*, meaning covered, and *graphie*, meaning writing. Therefore, steganography refers to methods of hiding secret data in other data such that its existence is concealed (Denning and Baugh, Jr., 1999). The obvious advantage of steganography as a tool for terrorist organizations and transnational criminal organizations is that information can be easily put on the Internet in plain view of the masses and government authorities but the true message is hidden. The most popular method of steganography is hiding information within an image known as Least Significant Bit modification (Rogers, 2005). Least Significant Bit modification takes the 1s and 0s from the secret message, that is, the payload, and inserts those into each pixel, starting at the bit least likely to make a noticeable change to the color of the pixel (Rogers, 2005). Also, steganography is not the only tool available for hiding data. There are a number of tools that can be used in addition to steganography and they are freely available on the Internet such as S-Tools, JP Hide-and-Seek, Gif-it-up, and Camouflage, just to mention a few.

Finally, another advantage of utilizing the Internet to launch cyber-attacks against the nation-state is the lack of regulation regarding Internet usage. According to Yar (2006), one of the greatest challenges facing government agencies is the fact that securing the Internet against potential cyber-attack is the absence of any centralized and coordinated regulation of the virtual environment.

In addition to using the Internet to launch a cyber attack against nation-states, terrorist organizations can use the Internet to carry out “hacktivism,” a combination of hacking and activism. The most common forms of hacktivism include, but not limited to, virtual sit-ins and blockades, email bombs, Website defacements, and viruses and worms. Virtual sit-ins are the equivalent of traditional protest method by which a particular site, associated with opposing or oppressive political interests, is physically occupied by activists (Yar, 2006). Email bombs are the tools used to overload email systems by sending mass mailings. This has the effect of overwhelming the system, thereby blocking legitimate traffic (Yar, 2006). Viruses, worms and other forms of malicious software are of limited use to hacktivists; still, they have been used by organizations worldwide. One such example of a devastating consequence of a malicious software attack occurred in 1989 against the U.S. National Aeronautics and Space Administration (NASA) when its computers became the target of the malicious worm known as the “WANK” worm (Figure 1), which stands for Worms Against Nuclear Killers (Yar, 2006). The hacker’s objective was to stop the launching of the shuttle that carried the Galileo probe on its initial leg to Jupiter. John McMahon, the protocol manager with NASA’s SPAN office, estimated the cost of the worm to be up to half a million dollars in wasted time and resources (Denning, 2001).

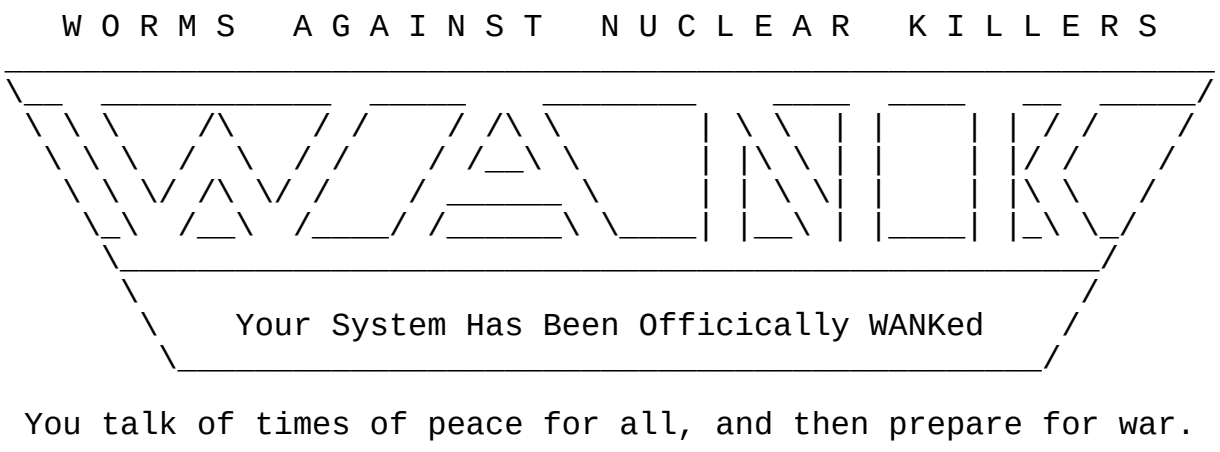


Figure 1: WANK Worm

During the first Gulf War, Israeli hackers launched virus attacks against Iraq's government systems in an effort to disrupt their communications capacity during the U.S. led invasion (Yar, 2006). The most recent example of the utility of cyber-attacks or cyber-warfare against a nation-state took place during the conflicts between Russia and Estonia (2007) and Russia and the Republic of Georgia (2008). According to the British news weekly magazine, *The Economist*, Russian nationalists who wished to take part in the attack on Georgia could do so from anywhere with an Internet connection, simply by visiting one of the several pro-Russia websites and downloading the software and instructions needed to perform a Distributed Denial of Service (DDoS) attack (The Economist, 2008). According to Verisign, a leading cybersecurity company, DDoS attacks direct large amounts of malicious traffic at online properties with the intent of causing the depletion or complete consumption of system- or process-critical resources, rendering services unreachable or unusable to their users. There are a variety of DDoS techniques that an attacker can and will use (See Figure 2). But no matter the form of the DDoS attack, its intentions are usually to disrupt a system in a way that prevents a legitimate user from gaining access to the system's operations. One form of DDoS, for example, is resource exhaustion. In this technique, the botmaster, the controller of the infected computer system, overloads the system to the point that it no longer responds to legitimate requests (Graham, Howard, and Olson, 2011).

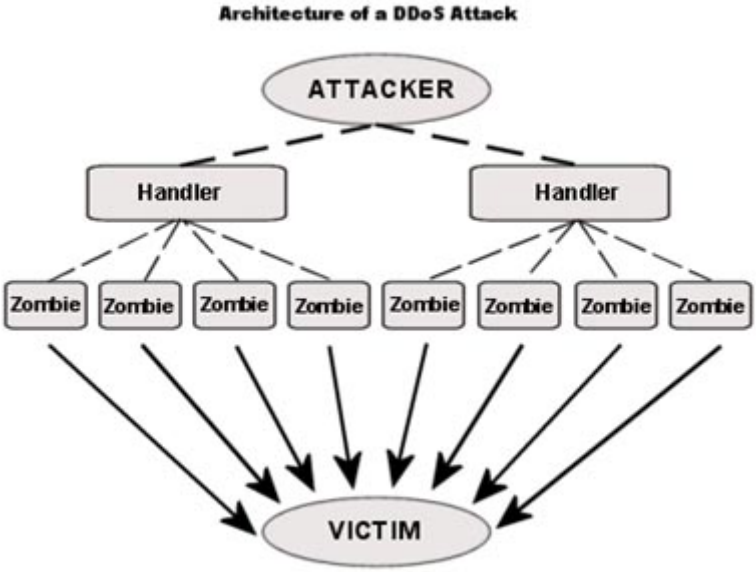


Figure 2: DDoS Attack

Source: http://niiconsulting.com/checkmate/2013/08/distributed-denial-of-service-ddos-attacks-know-thy-enemy/

The transition from terrestrial to virtual attacks offers a number of unforeseeable opportunities to terrorist groups against the nation-state. According to John Robb, a military futurist, the spontaneous, bottom-up mobilization of volunteer cyber-attacks in the Georgia conflict was an example of an open-source cyber-warfare, which has several advantages. "Leaving the attacks to informal cyber-gangs, rather than trying to organize a formal cyber-army, is cheaper, for one thing. The most talented attackers, with the best tools, might not want to work for the state directly. Best of all, from the state's point of view, is that it can deny responsibility for the attacks. It is the online equivalent of the use, by some governments, of gangs and militias to carry out attacks on political opponents or maintain control in particular regions" (*The Economist*, 2008).

Cyber-Terrorism Against the State

The concept of globalization, that is, the interconnectedness of the world as a result of great interdependence among nations, is comprised of and reliant on interconnected technological systems increasing the possibility of crimes against the nation-state. The concept of crimes against the state involves any activities that "breach laws protecting the integrity of the nation and its infrastructure (i.e. terrorism, espionage and disclosure of official secrets) (Yar, 2006). In the aftermath of the attacks of September 11th, 2001 targeting the Twin Towers in New York and the Pentagon in Washington, D.C., the United States took the lead in making legal provisions to protect the nation's computer systems against terrorist attacks (Yar, 2006).

Information Assurance (AI) has become a top priority of the United States Government in addition to data protection. Government agencies are also assuring information confidentiality, integrity, and availability (CIA Triad). According to McQuade, III (2006) Information Assurance became part of the lexicon of the U.S. government with the ratification of the President's Commission on Critical Information Infrastructure Protection (PCCIP) established in 1998 by Presidential Decision Directive 63. The PDD 63, the first national cybersecurity strategy, focused on critical infrastructure protection and public-private partnerships, and it created several information-sharing organizations such as the Information Sharing and Analysis Centers and National Infrastructure Protection Center (Negroponte and Palmisano, 2013). The President's Commission on Critical Information Protection is also responsible for protecting the nation's infrastructure which consists of "the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole" (McQuade, 2006). Former President George W. Bush also established the Comprehensive National Cybersecurity Initiative (CNCI). The CNCI called for "the development of an intrusion detection system and designated Department of Homeland Security to play the lead role in defending government networks, the implementation of a government-wide cyber counterintelligence plan, development of deterrence strategies, and the definition of the federal government's role for extending cybersecurity into critical infrastructure" (Negroponte and Palmisano, 2013).

The United States is also committed to protecting the homeland by utilizing the full legal force of Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, otherwise known as the USA PATRIOT Act. Enacted into law on 26 October 2001, the USA PATRIOT Act is also strengthened by provisions under the Computer Fraud and Abuse Act of 1984, including the

provision for life imprisonment of convicted cyber-terrorists (Yar, 2006). Recognizing the importance of securing cyberspace, former President George Bush released in February, 2003 *The National Strategy to Secure Cyberspace*. This 60-page document is part of an overall effort to protect the homeland and complements the *National Strategy for Homeland Security and National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*. According to *The National Strategy to Secure Cyberspace*, "cyberspace is the nervous system of the nation's infrastructure and it is comprised of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructure work" (*The National Strategy to Secure Cyberspace*, 2003).

The *National Strategy to Secure Cyberspace* (2003) articulates three strategic objectives and five national priorities. The strategic objectives are to prevent cyber attacks against America's critical infrastructures, to reduce national vulnerability to cyber attacks, and to minimize damage and recovery time from cyber attacks that do occur. The five national priorities include development of a National Cyberspace Security Response System, a National Cyberspace Security Threat and Vulnerability Reduction Program, a National Cyberspace Security Awareness and Training Program, a secure Governmental Cyberspace, and a National Security and International Cyberspace Security Cooperation.

The United States is also securing its cyberspace [1] by engaging in bilateral and multilateral diplomatic agreements with other nation-states. The United States is particularly concerned with the nature and extent of China's cyber activities and their implication for national security. In its latest report, *Red Cloud Rising: Cloud Computing in China* (2013) the U.S.-China Economic and Security Review Commission has once again called on the U.S. government to keep a watchful eye on the Chinese government's recent prioritization and development of cloud computing technology. According to the Report, three security issues are of concern to the U.S. and its national security:

> 1. Any future growth in US consumer use of China-based cloud computing infrastructure would likely raise significant security concerns. Regulations requiring foreign firms to enter into joint cooperative arrangements with Chinese companies in order to offer cloud computing services may jeopardize the foreign firms' information security arrangements. Furthermore, Chinese-language news sources indicate that China's primary foreign intelligence collection organization, the Ministry of State Security, has taken an oversight role in projects aimed at bringing foreign cloud computing investment to China.
>
> 1. Chinese cloud computing infrastructure could be used for offensive cyber operations, but the same is true of public cloud computing platforms globally. If Chinese public cloud infrastructure were ever to become unusually popular for these purposes, it would likely be due to a relative lack of oversight and lax enforcement of rules governing users' conduct by Chinese service providers, not due to Chinese cloud infrastructure being more "weaponized" than equivalent services in other countries.
>
> 1. The security vulnerabilities of Chinese cloud infrastructure are not inherently different from those of other cloud infrastructures around the globe. To the extent Chinese cloud infrastructure might on the whole be less secure, it would likely result from increased use of Chinese hardware and software (which, generally speaking, tend to have more security holes than their American counterparts), not from the fundamental design of that infrastructure (Ragland, McReynolds, and Southerland, 2013:1-2).

President Obama's International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World released May 2011 lays out the Administration's cyberspace policy. According to the

President's *International Strategy for Cyberspace*, the foundation of the United State's international cyberspace policy is the belief that networked technologies hold immense potential for the U.S. and the world. Therefore, the U.S. will pursue an international cyberspace policy that empowers the innovation that drives the U.S.'s economy and improves the lives of its citizens at home and those across the globe (*International Strategy for Cyberspace*, 2011). In his *International Strategy for Cyberspace*, President Obama recognizes that the U.S.'s armed forces must be prepared to face the military challenges of the twenty-first century in cyberspace. The use of bombs instead of bytes will always be the primary focus and mission of the U.S.'s military. However, the realities of conflicts in the twenty-first century dictate that in the wars of the future not only bullets but also bytes be an essential element for victory in the cyberspace battle field. As part of its military preparedness, the U.S., according to the President' *s International Strategy for Cyberspace* (2011), will adapt to the military's increasing need for reliable and secure networks, build and enhance existing military alliances to confront potential threats in cyberspace, and will expand cyberspace cooperation with allies and partners to increase collective security. One example of the U.S.'s cyberspace cooperation with its allies promoting collective security involves the Five Eyes: a technical cooperation program composed of Australia, Canada, New Zealand, the United Kingdom, and the United States.

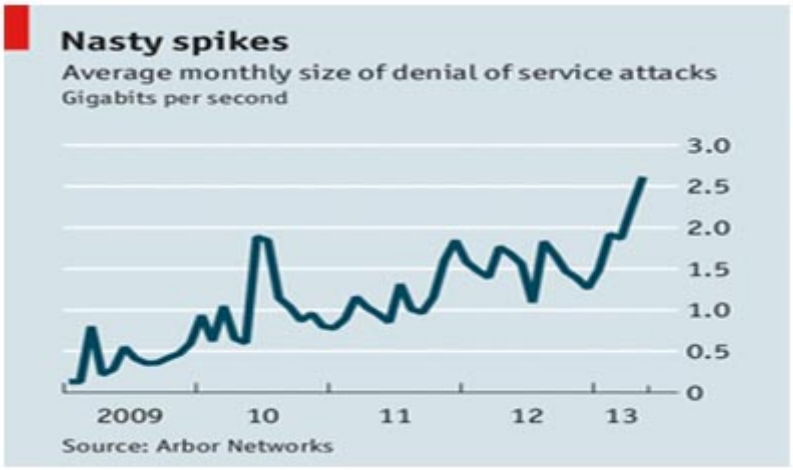
Implications and Policy Recommendations

The Department of Defense designated cyberspace a new domain of warfare in 2011. This elevation in strategic importance makes cyberspace comparable to land, sea, air, or outer space as a new battle frontier. The U.S. government and its armed forces recognize cyberspace as a potential future battleground. Former Defense Secretary Leon Panetta has publicly stated that, "cyberspace is the new frontier, full of possibilities to advance security and prosperity in the 21st century. And yet, with these possibilities, also come new perils and new dangers" (Panetta, 2012). The Chairman of the Joint Chiefs of Staff Army General Martin E. Dempsey stated that, "the Department of Defense is adding a new mission: defending the nation, when asked, from attacks of significant consequence—those that threaten life, limb, and the country's core critical infrastructure" (Roulo, 2013). For international jihadists the Internet has become without a shadow of a doubt the most cost-effective means of delivering its messages worldwide, coordinating attacks and, most importantly, the Internet allows jihadist organizations to recruit without leaving the confines of their safe havens. Jihadist groups and terrorist organizations are using the Internet as a tool to carry out their "cyberplanning" without fear of retaliation and in secret. Lieutenant Colonel Timothy L. Thomas, an analyst at the Foreign Military Studies Office in Fort Leavenworth, Kansas, defines "cyberplanning" as "the digital coordination of an integrated plan stretching across geographical boundaries that may or may not result in bloodshed" (Thomas, 2003).

As the Internet is assigned the importance of a domain as a new frontier in the battles of the twenty-first century, what can the U.S. government and its armed forces do to mitigate some of the potential disastrous consequences of a cyber-attack on the homeland. "Threats unseen are threats disbelieved," yet as former Defense Secretary Panetta has pointed out, foreign cyber actors are "probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electrical and water plants and those that guide transportation throughout the country" (Panetta, 2012).

First, the U.S. Department of Defense and its cyber security organizations (U.S. Cyber Command, Army Cyber Command, Navy Cyber Forces, and Air Forces Cyber/24th Air Force) must do everything within its power to stop or at least mitigate the consequences of Distributed Denial of Service (DDoS) attacks against the homeland's critical infrastructure. Army General Keith B. Alexander, Director of the National Security Agency, stated that "in August, the Saudi Aramco oil company was hit with a destructive attack that destroyed the data on more than 30,000 systems. In September, distributed denial of service attacks

began on the U.S. financial sector, and a few hundred disruptive attacks have occurred since" (Roulo, 2013). The Chairman of the Joint Chiefs of Staff Army General Martin E. Dempsey acknowledged that "intrusion attempts on critical civilian infrastructure systems have increased 17-fold over the last two years" and "the gap between cyber defenses deployed across critical infrastructure and offensive tools that now exists presents a significant vulnerability for our nation" (Roulo, 2013). Graph 1 shows the average monthly size of denial of service attacks.



Graph 1: Average monthly size of denial of service attacks

Source: The Economist, June 22, 2013.

Second, the U.S. Government should do everything in its power to shore up international support for the Budapest Convention on Cybercrime and other multilateral cybersecurity arrangements including, but not limited to, the International Telecommunications Union's World Summit on the Information Society (WSIS) and the Global Cybersecurity Agenda (GCA), the Asia-Pacific Economic Cooperation (APEC), the European Network and Information Security Agency (ENISA), the Computer Emergency Response Pre-Configuration Team (CERT-EU), and the NATO-Russia Council. This is an important step that should be taken by the U.S. Government and its cybersecurity agencies since the digital world routinely ignores national and international boundaries.

Third, the U.S. Government should provide the developing world technical and foreign aid assistance tied to the development of cyber investigation methods, cyber training, cyber policing, and law enforcement cooperation and assistance. The U.S. should do everything in its power to assist the developing world as it joins cyberspace as a latecomer. Perhaps the U.S. Government should create a Cyber Marshal Plan for the developing world similar to the Marshall Plan created for Europe in the aftermath of World War II when critical infrastructures were destroyed and the Plan helped in the reconstruction of Europe. The U.S. Government cannot afford to allow the developing world to become a conduit for cyberattacks against the homeland's critical infrastructure.

Fourth, the U.S. Government must continue to invest in its cyber workforce despite balance budget disputes and sequestration. As Frank J. Cilluffo, Director of the George Washington University Homeland Security Policy Institute, and Sharon L. Cardash, Associate Director Homeland Security Policy Institute, have stated, "there is no substitute for a human source (HUMINT). Collecting and exploiting all-source of intelligence is therefore the most robust way forward, even in the cyber realm" (Cilluffo and Cardash, 2013). However, Abraham R. Wagner, professor of International Relations & Public Affairs at Columbia University, pointed out, " while there is sound logic that shows there are increasing numbers of

jobs in cyberspace, the fact does not seem compelling enough to overcome the level of inertia in education today" (Wagner, 2012). In fact, thousands of jobs in the cybersecurity field – both in the government and private sectors – are going unfulfilled every year due to the lack of a trained computer workforce to satisfy the demand. The Chairman of the Joint Chiefs of Staff Army General, Martin E. Dempsey, should be applauded for this foresight into the nature of future conflicts in cyberspace and his pledge to hire 4,000 cyber operators to join the ranks of the U.S. Cyber Command over the next four years and to invest $23 billion dollar in cybersecurity.

Finally, the U.S. Government and its federal agencies must engage the private sector in a conversation regarding their shared responsibility and accountability for the exchange of information about cyber threats and cyber terrorism via the Internet. The Chairman of the Joint Chiefs of Staff Army General Martin E. Dempsey publicly acknowledged "sharing information about cyber threats is one of the most important ways to strengthen cybersecurity across the private sector but threat information primarily is shared in only one direction: from the government to critical infrastructure operators" (Roulo, 2013). With approximately 80 to 90 percent of critical technology infrastructure under the private sector supervision, private sector Chief Information Officers (CIOs) are in a unique position of leadership regarding the safety and welfare of the homeland. "They run the systems that need to be protected against terrorist threats" (Berinato, 2002). The cyberwar is a war that the U.S. cannot go alone. In this new domain the U.S. must be joined by cybersecurity industries in the private sector as well the international community. The Chairman of the Joint Chiefs of Staff Army General Martin E. Dempsey stated that "information sharing is just one path to safer network operations and others include improved cybersecurity standards and the establishment of internationally recognized rules for responsible behavior in cyberspace" (Roullo, 2013). Obviously, the U.S. Government and its allies must also do everything in their power to strike a balance between freedom of information and national security.

Conclusion

The image of terrorism that comes to mind when Americans think of "acts of terrorism," are usually the events of September 11, 2001 when 19 young men of Arab origin high-jacked four airplanes and flew two of them into the Twin Towers, one into the Pentagon, and one into a field in Pennsylvania. Hardly does one think of cyber terrorism or cyber attacks against the State in which its critical infrastructure are attacked via a computer virus or cyberattack by an enemy sitting half way around the world in a "rogue state" or "failed state" and out of reach of the arms of the law. Yet, as former Secretary of Defense Leon Panetta has stated, "a cyber attack perpetrated by nation states or violent extremists groups could be as destructive as the terrorists attack on 9/11" (Panetta, 2012).

Cyber-terrorism is a reality of the twenty-first century and for better or for worse it cannot be ignored. Audrey Kurth Cronin states that, "the Internet, an effective vehicle to spread civil society and democratic ideals, also provides a means to disseminate violent ideologies, coordinate criminal behavior, share combat tactics, research powerful weapons, and undermine traditional tools of order" (Cronin, 2013). As the Chairman of the Joint Chiefs of Staff Army General Martin E. Dempsey stated, "the spread of digital technology has not been without consequence. It has also introduced new dangers to our security and our safety" (Roulo, 2013). Ignore at our own peril. A cyber attack against the U.S.'s critical infrastructure by a terrorist organization, a transnational criminal organization, or a "lone wolf," acting on behalf of a rogue state from a safe haven and out of the reach of authorities could lead to a next "digital Pearl Harbor" (Panetta, 2012).

Notes

[[1]] The term *cyberspace* was coined by William Gibson (1982) and then popularized in his 1984 novel *Neuromancer*

, the term *cyberspace* became a popular descriptor of the mentally constructed virtual environment within which networked computer activity takes place (Wall 2008: 10).

References

al-Zawahi, A. "Letter from al-Zawahiri to al-Zarqawi," available at http://www.globalsecurity.org/security/library/report/2005/zawahiri-zarqawi-letter_9jul2005.htm. GlobalSecurity.org Accessed Monday, September 16, 2013.

Bamford, J. (2013). The Silent War. *Wired, July 2013: 90-99*

Berinato, S. Cybersecurity- The Truth About Cyberterrorism. March 15. 2002. Available at www.cio.com/article/print/30933

Cilluffo, F.J. & Cardash, S.L. (2013). Cyber Domain Conflict in the 21st Century. *The Whitehead Journal of Diplomacy and International Relations (Winter/Spring 2013): 41-47.*

Conway, M. (2002). What is Cyberterrorism? *Current History, 101(*659), 436-442.

Cronin, A.K. (2013). How Global Communications Are Changing the Character of War. *The Whitehead Journal of Diplomacy and International Relations*, Winter/Spring 2013: 25-39

Denning, D. E. (1999). Hiding Crimes in Cyberspace. *Information, Communication & Society, 2* (3), 251-276.

Denning, D. E. (2001). Cyberwarriors: Activists and Terroritsts Turn to Cyberspace. *Harvard International Review, 23*(2), 70-75.

Denining, D. E. (2001) Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *Computer Security Journal,* Vol. XVI, No. 4.

The Economist, "Internet Protests: The digital demo," June 29th, 2013: 56

Fleming, P. & Stohl, M. (2000) 'Myth and Realities of Cyberterrorism', paper presented at the International Conference on Countering Terrorism Through Enhanced International Cooperation, 22-24 September, 2000, Courmayeur, Italy.

Goldsmith, J. & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World.* New York, NY: Oxford University Press.

Graham, J., Howard, R, & Olson, R. (2011). *Cyber Security Essentials*. New York, NY: CRC Press.

"International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," May 2011 available at **http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf**

Knake, R.K. (2010). *Internet Governance in an Age of Cyber Insecurity*. Council Special Report No. 56, September 2010. New York, NY: Council on Foreign Relations.

Mueller, R. Testimony before the Senate Select Committee on Intelligence, January 11, 2007.

McCaughey, M. & Ayers, M.D. (Eds.) (2003). *Cyberactivism: Online Activism in Theory and Practice*. New York, NY: Routledge.

McQuade, III. S.C. (2006). *Understanding and Managing Cybercrime.* New York, NY: Pearson.

Negroponte, J.D. & Palmisano, S.J. (2013). *Defending on Open, Global, Secure, and Resilient Internet.* New York, NY: Council on Foreign Relations

Panetta, L. Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, October 11, 2012. Available at http://www.defense.gov/utility/printitem.aspx?print=http://www.defense.gov/transcripts/transcript.aspx?transcriptid

Ragland, L.A, McReynolds, J. & Southerland, M. (2013). *Red Cloud Rising: Cloud Computing in China.* Available at http://origin.www.uscc.gov/sites/default/files/Research/DGI_Red%20Cloud%20Rising.pdf

"Remarks of the President on Securing Our Nation's Cyber Infrastructure," While House, May 29, 2009, available at **http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure**.

Rogers, R. (2005). *Hacking a Terror Network: The Silent Threat of Covert Channels*. Rockland, MA: Syngress Publishing, Inc.

Roulo, C. DOD Must Stay Ahead of the Cyber Threat, Dempsy Says. U.S. Department of Defense. Available at **http://www.defense.gov/news/newsarticle.aspx?id=120379**

Roulo, C. Nation Must Defend Cyber Infrastructure, Alexander Says. U.S. Department of Defense. Available at http://www.defense.gov/news/newsarticle.aspx?id=120391

Shinder, D. "Extreme cybercrime: preparing for the worst," available at **http://www.techrepublic.com/blog/it-security/extreme-cybercrime-preparing-for-the-worst**. Accessed Monday, September 16, 2013.

Schmidt, E. & Cohen, J. (2012). *The New Digital Age: Reshaping the Future of People, Nations and Business.* New York, NY: Alfred A. Knopf.

Theohary, C.A. & Rollins, J. Terrorist Use of the Internet: Information Operations in Cyberspace. Congressional Research Service (CRS Report R41674).

The 2008 Annual Report to Congress of the U.S.-China Economic and Security Review Commission available at http://www.uscc.gov/index.php. Accessed November 23, 2008.

The National Strategy to Secure Cyberspace, February 2003. Available at **http://www.us-**cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

The Economist. (2008). Marching off to cyberwar. Available at **http://www.economist.com/science/tq/displaystory.cfm?story_id=12673385**. Accessed on December 5, 2008.

Verisign (2012). Distributed Denial of Service (DDoS) Attacks: Evolution, Impact & Solutions.

Verton, D. (2003). *Black Ice: The Invisible Threat of Cyber-Terrorism.* Emeryvill, CA: McGraw-Hill.

Wagner, A.R. (2012). Cybersecurity: From Experiment to Infrastructure. *Defense Dossier Issue 4 (August 2012): 16-20.*

Wall, D.S. (2008). *Cybercrime.* Malden, MA: Polity Press.

Yar, M. (2006). *Cybercrime and Society.* Thousands Oaks, CA: SAGE Publications Ltd.

All views are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government.

About the Author

José de Arimatéia da Cruz

Dr. José de Arimatéia da Cruz is a Visiting Research Professor, U.S. Army War College, Carlisle Barracks, Carlisle, PA. He is also a Professor of International Relations and Comparative Politics, Department of Criminal Justice, Social & Political Science, Armstrong Atlantic State University, Savannah, Georgia. He holds a Ph.D. in Political Science, Miami University, Oxford, Ohio; M.A. in Political Science/Political Philosophy, Miami University, Oxford, Ohio; M.S. in Criminal Justice (Cyber Affairs and Security) Armstrong Atlantic State University, Savannah, Georgia; and B.A. in Philosophy, Wright State University, Dayton, Ohio. He has published in the *Journal of Politics & Policy*, *Studies Revue Canadienne des Etudes Latino-Americaines et Caraib*, *Law Enforcement Executive Forum*, *International Social Science Review*, *The Latin Americanist*, *Latin American Politics and Society*, and *Journal of Third World Studies.*

Available online at : http://smallwarsjournal.com/jrnl/art/terrorism-war-and-cyber-insecurity

Links:
{1} http://smallwarsjournal.com/author/jos%C3%A9-de-arimat%C3%A9ia-da-cruz
{2} http://niiconsulting.com/checkmate/2013/08/distributed-denial-of-service-ddos-attacks-know-thy-enemy/
{3} http://www.globalsecurity.org/security/library/report/2005/zawahiri-zarqawi-letter_9jul2005.htm.
{4} http://www.cio.com/article/print/30933
{5} http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
{6} http://www.defense.gov/utility/printitem.aspx?print=http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136
{7} http://origin.www.uscc.gov/sites/default/files/Research/DGI_Red%20Cloud%20Rising.pdf
{8} http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure
{9} http://www.defense.gov/news/newsarticle.aspx?id=120379
{10} http://www.defense.gov/news/newsarticle.aspx?id=120391
{11} http://www.techrepublic.com/blog/it-security/extreme-cybercrime-preparing-for-the-worst
{12} http://www.uscc.gov/index.php
{13} http://www.us-
{14} http://www.economist.com/science/tq/displaystory.cfm?story_id=12673385
{15} http://smallwarsjournal.com/comment/reply/14792#comment-form