Cyber Warfare:
A Misrepresentation of the True Cyber Threat

by Troy E. Smith, Trinidad & Tobago

Abstract

The reliance by contemporary society on computers and computer-based systems has increased exponentially over the last twenty years. Technology now forms an essential part of every country's critical infrastructure and is, therefore, a major national security concern. This concern, combined with the complexity of cyberspace and political agendas, has caused a misrepresentation of the cyber threat. Although the motivation for cyber-attacks has only been associated with criminal behavior, espionage, and even terrorism, current administrations and the media would have the country believe that cyber war is upon us. This article demonstrates that cyber war is certainly a misnomer. To date there has been an inability to acquire any substantial, irrefutable evidence of cyber warfare, only speculations based on historical information, rumors, propaganda, and misinterpretation or misrepresentation of facts. Current international legal frameworks and interpretations indicate that what has been termed cyber warfare does not match the criteria for war. While the dispute over the term cyber war and what it represents will definitely continue, there is consensus on the reality of cyber weapons and cyber-attacks. Although these weapons cannot be described by definitions that have been developed for classical weapons, they still can pose a real potential threat. The continued misrepresentation of the cyber threat can lead to loss of support by citizens and stakeholders, who will claim the administration cried wolf. The loss of support would stymie the development and implementation of activities to prevent, mitigate, and raise awareness about the cyber threat.

> The clever combatant imposes his will on the enemy, but does not allow the enemy's will to be imposed on him.
>
> - Sun Tzu

In an age where the reliance on computers and computer-based systems has grown exponentially, technology now forms a vital part of every country's critical infrastructure. The increased reliance on computers has led to them becoming a target for attack. These cyber-attacks encompass acts of protest, crime, vandalism, espionage, and terrorism. Additionally, the cyber war was added to the list; this term has grown in popularity of late. However, countries, policymakers, information technology experts, national security agencies, and the military have expressed widely different opinions regarding previous cyber security incidents adding up to war. Some people refer to the threat as a looming "Cyber Pearl Harbor," while others simply state that "cyber war will not take place." While there has been controversy over the term "cyber war" and what it represents, there is consensus on the reality of cyber weapons and cyber-attack. As more people began to appreciate the cyber threat, activities to prevent, mitigate, and raise awareness have increased.

Nevertheless, while generally the motivation for cyber-attacks has been related to criminal behavior, espionage, and even terrorism, some agencies believe that war is on the horizon. In 2011 the Pentagon declared that cyber-attacks would act as *casus belli* (cause for war). While this stance may intimidate potential hackers, one agency saying that something is *casus belli* is inadequate in the international realm. Interpreting cyber-attacks as a type of aggression or equating them to the use of force in lieu of the United Nations Charter is inconclusive and a legal consensus is not expected soon.[1] The UN Charter permits the use of force only in two circumstances, when the UN Security Council authorizes it or, under Article 51, in a case of self-defense. In Article 51, the inherent right to self-defense is as a result of an armed attack. There is an interpretation in international law that talks about anticipatory self-defense. Law professor and retired general Charles Dunlap says that anticipatory self-defense means "retaliation is justified only where the necessity of that self-defense is instant, overwhelming, and leaving no choice of means and no moment for deliberation." Thomas Rid has said, "Cyber-war lacks the essential characteristics to meet the conditions of becoming an act of war; if the use of force in war is violent, instrumental, and political, then there is no cyber offense that meets all three criteria." Rid's view that it is improbable that cyber-attacks will become an act of war has been supported by specialists at the Center for Strategic and International Studies.

On the other end of the spectrum there are many who say, "We should head for the hills; the cyber war is not coming, it's here." Justification for their stance on cyber warfare

comes from their interpretation of various cyber events. One prime example, though perhaps the only allegedly successful one, was the sabotaging of the Soviet Urengoy-Surgut-Chelyabinsk natural gas pipeline in 1982. According to Thomas C. Reed, "The CIA procured a modified pipeline control system in anticipation of KGB trying to steal it." The result was supposedly a massive explosion after the eventual malfunction and pump reset.[2] Although this incident seems significant, there are multiple factors that negate its importance. First, it is not "true" cyber warfare, as it requires physical involvement for it to be used and to be effective. Secondly, one of the key reasons why cyber-attacks are used is to prevent the attacker from being irrefutably identified and lending to war; this is the problem of attribution. The ease of performing acts anonymously in cyberspace through concerted efforts to conceal one's identity makes proving an entity's involvement both difficult and time-consuming. Stuxnet, which is considered the best example of a warlike application of a cyber-attack, has yet to be attributed to any person or nation. There has been an inability to acquire any substantial, irrefutable evidence; only speculations based on historical information, rumors, and propaganda have come forward.

> One of the most discussed and possibly overemphasized cyber-attacks is the Distributed Denial of Service (DDoS). I say overemphasized because the actual threat that this type of attack poses is not as extensive as it may seem at a cursory glance. Firstly, the DDoS is a blunt tool that in essence floods an Internet address with data in hopes that the server will "clog" and shut down. As such it serves very little purpose in most case scenarios; internal networks are immune to such attacks by design and hence institutions core to the national interest and security are essentially safe. Furthermore, as quickly as DDoS attacks grew in popularity, relevant specialists developed countermeasures. While no clear solution has been found, one can choose from simple switches to block surges in internet traffic, through renting secure tunnels, to complex blackholing (passing the incoming data through a selective filter) provided by some companies (Struglinski, 2012).

While DDoS attacks have become a popular cyber weapon, Stuxnet worm trumps DDoS in complexity, effectiveness, and dispersion (albeit seemingly a side effect rather than an attribute). Subsequent to the alleged use of Stuxnet by Israel, this type of cyber-attack has been thought of as the future of warfare. Stuxnet was engineered to exercise surgical precision to find and affect its specific target.[3] While the general belief is that the cyber-attack was aimed at destroying industrial equipment, specialists insist that it was designed to sabotage the system for an extended period. The glory of Stuxnet was much like a shooting star; while bright it was short-lived. This was because the effectiveness of the Stuxnet worm, as with other worms, was dependent on it remaining undetected. Much like the worms and viruses that can attack one's personal computer, once it is discovered antivirus solutions are quickly developed. Within a short time of being discovered, Stuxnet was neutralized. Additionally, once the virus is discovered it will be analyzed, and the flaw in the network infrastructure it utilized will be fixed by patches developed by computer security specialists. Effectively, not only is the virus itself "a one-bullet gun" but so is the method it utilizes, meaning every time a new flaw must be found to exploit. Furthermore, anyone who has completed the GIAC Certified Incident Handler (GCIH), which has been added to the CND Analyst category of Department of Defense Directive 8570 (DoD 8570), knows that normally direct access to the network or a computer which accesses the network is essential. This is normally gathered through physical entry into the compound or by profiling employees and tricking them into putting the virus on the system or at least helping to create or identify a "backdoor" for its entry. Since this was not possible in this case, the worm had to take an indirect route. The cyber-attacker had to allow the worm to infect multiple systems in the hope of it reaching the target system. A weapon relying on chance requiring extended periods of time to take effect, and which cannot be used overtly and is capable of striking only once, can hardly be considered a particularly threatening one at this stage.[4]

To capitalize on the potential of cyber-attacks, they must be covert and anonymous.

To capitalize on the potential of cyber-attacks, they must be covert and anonymous. First, for the cyber-attack to hit its target it must remain hidden and be allowed time to do damage. Therefore, open war will hinder the effectiveness of the cyber-attack, as during this time operations security and information security measures will be heightened, making penetration of networks extremely difficult. Second, this nature of anonymity allows for nations to engage in espionage with little chance of armed or legal retaliation and the Clausewitzian escalation. Even though the U.S. has taken a stance that cyber-attacks are *casus belli*, without a clear enemy a retaliatory cyber offensive cannot occur. Furthermore, without the ability to precisely identify an attacker and prove his/her involvement, international support would be terribly difficult to obtain for any retaliatory action. As such, cyber does not align itself with war as currently defined, but is much more akin to intelligence operations. Additionally, following the Clausewitzian concept, although Stuxnet had a political component (e.g., forcing the Iranians to return to negotiations), the lethal component was missing. Even if

lives were lost in these attacks, the principal aim was sabotage, an "accepted" act in the international arena and a form of political warfare, not war and death itself.[5]

The Clausewitzian theory of war would suggest that most cyber-attacks in the political sphere should be categorized as sabotage or espionage.

The idea of cyber-attacks equating to conventional warfare is controversial in its legal accuracy, severity, lack of precision, motivation, and inability to support multiple usage. Events to date and contributions of technology experts lead us to believe that based on current infrastructure most cyber-attacks can be described as Weapons of Mass Annoyance.[6] Stuxnet, which many consider as a prime example of the potential of cyber warfare, did not have the fast, direct, and precise effect on its target as expected of a weapon of war. While in this case the desired effect was obtained, due to its indirect nature and the lack of control once released, Stuxnet action could not be coordinated with any other action. The indirect nature of cyber-attacks combined with the fact cyber-attacks lack repeatability, as systems can be adapted to defend against the specific attack after one encounter, make them a poor choice in war situations. The effects of cyber-attacks are not sufficient in duration and severity to be considered a serious attack. The Clausewitzian theory of war would suggest that most cyber-attacks in the political sphere should be categorized as sabotage or espionage. Acts of sabotage and espionage which have been used during and before wars have traditionally not been considered an act of war in themselves and hence are not *casus belli* in international law. If espionage is an act of war, then America would be at war even with its allies. If the main use of cyber-attacks by state actors remains espionage or is limited to espionage due to limitations of cyber-attacks, there is no basis for considering cyber-attacks as being *casus belli*.

The current international legal framework and interpretations indicate that what has been termed cyber-warfare does not fit the criteria for war. However, the concept of cyber-weapons is more acceptable. Although these weapons cannot be described by concepts we have developed for classical weapons, they still can pose a real potential threat. Cyber-weapons are different from classical ones, in that they are not directly lethal; however, if used correctly they can lead to potentially lethal situations and devastate economies. If used as a diversionary tactic they could facilitate other physical attacks, related to classical wartime activities. Providing corrupted software and hardware to an enemy is a possibility given current security measures, and this ability only increases during the chaos of war. The true potential effect of cyber-attacks comes from their strategic impact and the immense power an individual can yield with just a few keystrokes due to their asymmetric nature. In addition, cyber-attacks possess the frightening ability to strike without warning from varying distances, which can be as far as continents apart. Therefore, it is probable that cyber-attacks in the political sphere will continue to be used where their strength lays, in intelligence collection, espionage, and sabotage.

If the cyber-war is not real, why give it so much attention? Should not the focus be on the real threats of cyber crime and cyber espionage? To a large degree it seems cyber-attacks have been sensationalized by the media, creating the idea of a cyber war. It should also be noted that most, if not all, reports that "confirm" the looming cyber war are from for-profit companies, which are mainly concerned with selling a product. Identifying the source of the potential cyber war, and developing countermeasures for it, is a rapidly expanding industry, which has private companies clamoring for a piece of the pie. The Obama administration has allowed and actually joined the call for preparedness against a cyber war. However, this does not necessarily validate the concept of cyber war; rather it can be interpreted as a political scam on the part of the administration. The goals of this misinformation are two-fold. First, the administration aims to pressure the Congress into passing cyber security legislation. The exaggeration of the threat can act as a serious motivating factor for the Congress to take action. Appeals to emotion such as fear can invoke a considerably faster response compared to debate. Second, the administration wants to get the public to inadvertently buy in to its reining in the generally unregulated Internet. This will give the government greater control over the Internet. This scam can be compared to the USA PATRIOT Act, which was introduced when Americans were injured and in deep fear of terrorist acts, and were primed to accept anything the administration said would aid in preventing another 9/11. However, once that time had passed and citizens began reviewing the Act analytically, they realized that it actually infringed on their constitutional rights and gave the administration and the intelligence community a new, unchecked power, which could be easily abused.

The true problem in the wrongful association of cyber-attacks with war is that we can create a self-fulfilling prophecy. Already, as a result of the interpretation of cyber-attacks being possible acts of war, there has been increased tension between Russia and China, and with the Western powers. In addition to this, as each nation attends to the idea of an approaching cyber war, it is dedicating resources not only to defend against an attack but also to develop powerful cyber weapons that could be utilized in a cyber

war. Also, instead of the likely overreaction that may occur on the part of government, the misrepresentation of the threat may lead to its outright dismissal. After people continue to hear "wolf" cried for too long they might dismiss the threat of cyber war and, unfortunately, the reality of the cyber threat along with it. Future administrations must make concerted efforts to develop the necessary policy instruments and review the applicability of current international law, rather than merely propagate the concept of cyber war.

Notes

[1] Waxman, Matthew C., "Cyber-attacks and the use of force: Back to the future of article 2(4)," *The Yale Journal of International Law* 36, no. 2, 2011: 421-459.

[2] Reed, Thomas C., and George Bush, *At the abyss: An insider's history of the cold war*, New York: Random House Publishers, 2004.

[3] Last, Jonathan V., *How the Worm Turned: Stuxnet versus the Iranian nuclear program*, December 13, 2010, http://www.sodahead.com/united-states/have-you-heard-of-stuxnet-if-not-you-really-need-to-read-this/question-1379899/ (accessed July 13, 2011).

[4] Struglinski, Damian, *How Serious Is the Threat of Cyber Warfare?* London: King's College University, 2012.

[5] Gady, Franz-Stefan, "A Reality-Based Model for Cyber Conflict," *EastWest Institute*, 2012, http://www.ewi.info/reality-based-model-cyber-conflict (accessed June 8).

[6] Lewis, James Andrew, *Assessing the risks of cyber terrorism, cyber war and other cyber threats*, Washington, DC: Center for Strategic & International Studies, 2007.

Troy E. Smith, a citizen of the Caribbean nation of Trinidad and Tobago, entered the field of intelligence in 2008 upon joining the Security Intelligence Agency of that country. His initial position was as an intelligence officer, for which he was trained as an analyst and in tradecraft for possible field work. Subsequently, he embarked upon several training endeavors, to include a 3-week course hosted by the CIA. As an analyst he has written a number of papers on the intelligence activities of the Chinese. After beginning the MA in Intelligence Studies degree program at American Military University in the U.S., he developed an interest in cyber crime and cyber warfare. He is currently writing an article on motivations for cyber crime with Johnathan Clemens. Mr. Smith now serves as the Operations Security Manager for his nation's Strategic Services Agency. He has recently completed the Agency's OPSEC plan and presented a paper to its executive leadership on the insider threat.