2013 5th International Conference on Cyber Conflict
K. Podins, J. Stinissen, M. Maybaum (Eds.)
2013 © NATO CCD COE Publications, Tallinn

Cyber Attack: A Dull Tool to Shape Foreign Policy

Emilio Iasiello
iSight Partners
iasiello@aol.com

Abstract: This paper examines how cyber attacks, if indeed conducted by nation states, have been unsuccessful in supporting states' foreign policy objectives. By analyzing three prominent case studies, I show that as a result of geopolitical tensions, cyber attacks were implemented to further nation state objectives in support of foreign policy considerations and failed to achieve their respective outcomes despite successful deployment against their intended targets. The three case studies, hypothetical scenarios because attribution has not been confirmed, include: (1) the October 2012 distributed denial of service attacks targeting the U.S. banking sector; (2) the 2012 Stuxnet attack against Iran; and (3) the 2007 cyber attacks against Estonia. I work with the assumption that nation states were orchestrating the attacks through proxies, or else were actual participants, based on intent, motive, and a plethora of circumstantial evidence presented in each scenario. Data has been collected from newspapers, information technology security periodicals, and expert analysis. This paper challenges the notion that states can use the threat of cyber attack to influence an adversarial nation state's behavior, much the same way the threat of nuclear weapons holds other states in check.

Keywords: *cyber attack, DDOS, Stuxnet, Estonia, Iran, foreign policy*

1. INTRODUCTION

In 2007, the Internet security company McAfee published a report citing that approximately 120 countries already possessed or were developing capabilities to conduct offensive cyber operations.[1] Ostensibly, such capabilities would enable a nation state to perform cyber attacks or conduct cyber espionage at home or abroad against adversaries and allies alike, depending on the intent. Since the publication of that report, there have been several world events that have demonstrated a different, more strategic purpose behind cyber attacks: use as a tool to exert control and gain political influence. In particular, the 2007 distributed denial-of-service attack against Estonian government networks; the 2012 unofficial acknowledgement by a senior government official of the United States involvement in deploying Stuxnet and Flame (and possibly Duqu and Gauss) against a network controlling Iranian nuclear centrifuges, as well as other Middle Eastern networks;[2] and the 2012 DDOS against U.S. financial institution networks hint of nation state direction and/or involvement based on intent, target selection, and the desired effect created. Why these events are significant is that a deeper motivation lurked beneath the perpetrators' intent to just disrupt, deny, degrade, or destroy information systems or the information resident on them; these attacks were designed to create opportunities and influence events to gain political advantage. However, while it can be argued that these cyber attacks succeeded in accomplishing their tactical missions, they ultimately failed in their strategic objectives. At present, authoritarian governments such as China and Iran have achieved some modicum of success using offensive cyber operations to monitor and censor hostile information from reaching its public, or identifying and targeting political dissident and oppositionist groups that pose a threat to regime stability. Yet even the most draconian restraints are subject to circumvention by the more technically savvy and diligent oppositionists, reducing the overall effectiveness of these technical measures. More importantly, the capability to exert influence over an indigent populace does not hold the same authority as being able to use the same capabilities to influence decision makers in a country next door, no less one thousands of miles away. Whereas nuclear weapons have been used as the platforms from which nuclear states have flexed diplomatic muscle, cyber weapons have not yet reached that revered plateau. To date, cyber weapons have failed to wreak the awe inspiring havoc of their nuclear counterparts and thereby cannot be used as a saber rattling tool of foreign policy. Until such a time, cyber weapons will continue to be more terrifying in theory than practice, and remain a pejorative sound bite used by politicians and military hawks as the harbinger of future threats than an effective policy prescriptive tool for today's governments and militaries.

2. NUCLEAR WEAPONS VS CYBER WEAPONS

Ever since the two atomic bombs were dropped on Hiroshima and Nagasaki, the world has been privy to the devastating effects of nuclear weapons. In 1945, a yardstick had been inadvertently established that would forever become the benchmark for future nuclear weapons development. Superpowers now had a standard by which to convey their might to their adversaries. The implied threat was clear: cross any “red lines” and an assured destruction would take place. The Cold War ushered in a near twenty-year global race for nuclear supremacy. What capability one country had, competitors and allies alike wanted as well. Since 1945, eight countries are believed to have some level of nuclear weaponry; one is believed to have weapons although has not publicly acknowledged it; and in the case of Iran, one may or may not be actively trying to develop them.

Most nuclear states will readily admit that the reason for possessing such a capability is largely to deter the potential hostile actions of their enemies. Nuclear weapons, or the very threat of their acquisition, have succeeded in bringing powerful nations to the diplomatic table. North Korea has consistently used the threat of nuclear weapons development as a bargaining chip to achieve tactical objectives such as receiving food and humanitarian aid. Israel’s assumed possession of nuclear weapons has helped enable it maintain its strong position in the Middle East, and Iran’s pursuit of this capability can be interpreted as its attempt to gain regional supremacy and create a level playing field with its main adversary, Israel. Nuclear deterrence theory is largely rooted in the fact that a nation state has the capability and credibility to deploy nuclear weapons as does its adversary, thereby creating a military stalemate.

As cyber claims the prize as the 21st century’s greatest non-nuclear threat, many experts and influential people such as U.S. Cyber Command’s General Keith Alexander and former deputy assistant director for the FBI’s Cyber Division Steven Chabinsky believe that offensive actions can be applied to this asymmetric domain to deter hostile adversarial actions in cyberspace. The United States in particular has taken initiatives in getting its military involved in addressing the cyber problem. In May 2011, the White House released its *International Strategy for Cyberspace* outlining how it would approach its use of cyberspace, promoting its core commitments to fundamental freedoms, privacy, and the free flow of information. While not explicit, the strategy states that the U.S. “reserves the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law.”[3] What can be inferred from this is U.S. intent to employ whatever tools at its disposal to defend itself, its allies, its partners, and its interests. In July 2011, the U.S. Department of Defense released its *Strategy for Operating in Cyberspace,* which clearly articulated the role of the U.S. military to ensure that it has the necessary capabilities to operate effectively in the cyberspace, citing it as a military domain much like air, land, and maritime,[4] with U.S. Cyber Command leading the efforts to "conduct full-spectrum military cyberspace operations to ensure U.S. and allied freedom of action in cyberspace, while denying the same to their adversaries."[5] Whether it wants to admit it or not, like in the nuclear domain, the United States has taken the first step toward militarizing cyberspace.

However, as several articles and publications attest, there is no cyber equivalent to nuclear deterrence, based largely on four factors: 1.) Nation states typically do not assume responsibility for hostile actions taken in cyber space; 2.) There has been no awe inspiring, game changing, show of what a cyber attack can do; 3.) Attribution in cyberspace is extremely difficult and can't be as precise as identifying a nation state that has launched a nuclear weapon, and 4.) Unlike nuclear weapons development, which can be monitored, there is no similar transparency for nation state production of cyber weapons, nor an international watchdog agency to track such developments. These actions ultimately hinder nation states from applying a similar mutual assured destruction concept to cyberspace. Therefore, as the following case studies will demonstrate, nation states using cyber attacks to support foreign policy objectives will ultimately fail to effectively influence decision makers into favorable courses of action, or deterring political and/or military actions.

3. HYPOTHETICAL CASE STUDIES

These hypothetical case studies show how suspected nation state cyber activity was used in the hopes of obtaining a political objective outside its tactical mission. To date, there has been no definitive nation state attribution or linkage to these case studies. While attribution in cyberspace is nearly impossible, certain elements such as actor motivation, intent, behavioral actions, actor profiling can be identified, evaluated, and assessed to help better understand the significance of these cyber events – not just from an operational level, but from a strategic perspective as well.

A. *2007 ESTONIA DISTRIBUTED DENIAL-OF-SERVICE ATTACK*

Note: It is difficult to discuss the 2007 cyber attacks against Estonia without bringing up the 2008 distributed denial-of-service (DDoS) attacks directed at Georgia. While both cyber campaigns were suspected instruments of the Russian government conducted through proxies, they differ in that the 2008 attacks were conducted in tandem with the invasion of Georgia's Ossetia region by Russian armed forces. I assume the premise that the Russian government had at least an informal role in directing the activity. Therefore, if the Russian government was involved, and the DDoS activity was an instrument of its foreign policy, its objective could be construed as an attempt to influence an Estonian government course of action favorable to Russian interests.

In late April 2007, Estonia relocated a Soviet-era bronze statue and inadvertently opened a virtual Pandora's Box of cyber malfeasance against its national networks. For three weeks, Estonia was the victim of politically-motivated cyber attacks targeting websites of political parties, and distributed denial-of-service (DDoS) attacks against governmental, and commercial organizations to include schools, Internet service providers, media channels, and private websites.[6][7] Given that Estonia has long been considered a modern nation and among the most wired countries in the world, this was a serious concern. A flummoxed Estonia searched for courses of action, enlisting international support to mitigate the cyber attacks. The world was witness to what it had long heard about but up until this point had never seen – cyber attacks shut down a country's information infrastructure.

1) *It Was The Russians...I Think*

Bilateral tensions between Russia and Estonia are deep rooted and have been festering for over eighty years. From 1918 when Estonia first gained its independence from Russia until 1991 when it regained its ultimate independence, Estonia has viewed Russia's presence as an illegal occupation.[8] Moscow's attempts to "Russify" Estonian culture has been compounding this friction, relocating hundreds of thousands of ethnic Russians to Estonia starting in 1940 and continuing throughout the Cold War.[9] Suffice to say, foreign relations between these two countries remain a constant work in progress, ebbing and flowing according to the diplomatic and political environments. Estonia's relocation of the Soviet war memorial from the center of Tallinn to a military cemetery in 2007 was the catalyst for physical and digital protests. At the time, Estonia had a substantial Russian-speaking population, almost a third of Estonia's population of 1.3 million.[10] Patriotic hackers and established Russian youth groups who had previously engaged in hostile cyber activity against Chechen websites,[11] immediately mobilized to defend Russian nationalist interests. Clearly Russian government reaction to the Estonian government was bold and resolute, threatening to sever diplomatic relations and calling Estonia's statue removal as "blasphemous and barbarous."[12] The scene was set – a showdown between a powerful nation state and its smaller, younger, and highly individualistic cousin.

So why a cyber attack?

The 2007 cyber attacks against the Estonian information infrastructure can be interpreted as an instance where a nation state tried to influence the decisions and actions of another country using cyber weapons. The three-week long DDoS achieved several different outcomes including the expression of diplomatic discontent; the flexing of "virtual" muscles; and the capturing of the Estonian government's attention. More importantly, the world observed firsthand the potential consequences of a serious cyber attack.

- **Expressing Diplomatic Discontent**: The fact that the Pro-Kremlin youth group "Nashi" immediately claimed responsibility for the cyber attack was a signal to the Estonians that the Russian government may have had influence on the group allegedly behind the attacks, if only as the puppet master pulling the strings. Nashi had an established track record of working on behalf of Moscow to include spying on other youth groups and conducting DDoS against unfriendly newspapers.[13] Furthermore, a State Duma official acknowledged a relationship with a Nashi "commissar intimating a possible collusion between the Russian government and this group with regards to the attack.[14] So the message was clear: While it couldn't be proven, the Estonians and the rest of the world for that matter saw Russia's hand in this attack.
- **Flexing "Virtual" Muscle**: The DDoS did not target a sector or a specific organization but a *nation's information infrastructure*. This wasn't a mistake or a serendipitous happenstance, rather, a calculated, planned operation that systematically executed an attack that increased in intensity throughout its duration. As one of the most wired countries in the world, a potent DDoS disrupting but not destroying key services seemed to be sending a potent message: "If our youth group hacktivists can do this to you, imagine what the full fury of the Russian government can do?" Up until that point, DDoS attacks had been primarily used by hacktivists and patriotic hackers to express discontent, but none had ever achieved the magnitude of these attacks.
- **Capturing Estonia's Attention**: The DDoS attack can be considered a virtual "slap" to get Estonia back in line. The fact that the DDoS ended as quickly as it had started further supports the fact that it was a measured response designed to make a statement, rather than cause permanent or irrevocable damage. So the intent was not to bring down the system, which could have easily been done. Russia initially postured, threatening to sever diplomatic relations as a result of the statue's relocation, suggesting that if the statue were replaced, diplomatic relations would be reinstituted. When physical protests did nothing to dissuade the Estonian government, DDoS attacks quickly targeted government networks at the onset. Throughout its duration, the DDoS increased in intensity, particularly on days of historic significance, such as the

on May 9 – “Victory Day” in Russia commemorating the capitulation of Nazi Germany to the Soviet Union in 1945.

2) *But Did It Work?*

Clearly from a tactical standpoint, the DDoS attacks against the Estonian information infrastructure were an unqualified success. For three weeks, Estonia was the target of these attacks. Each time there was a pause in the activity, it would resurface soon after stronger and more potent than earlier iterations. What’s more, the attackers constantly tweaked their malicious server requests to evade filters.[15] More lasting damage could have been done but wasn’t.

Estonia remained resolute and did not surrender or acquiesce to Russia’s demands. Instead, Estonia solicited international support in mitigating the cyber attacks. Estonia’s unique situation encouraged NATO to consider the repercussions of cyber attacks when directed against a nation state, incentivizing NATO’s creation of a cyber center of excellence to improve NATO’s cyber defense posture.

If involved, Russia may have correctly anticipated NATO’s reluctance to consider enacting Article 5 and opting to provide defensive network support instead of escalating the situation by rallying NATO members behind Estonia. Although Russia, if they were involved, might have estimated this course of action correctly, it was not a guaranteed outcome. At the time, while there was no precedent to addressing a state-level cyber attack, NATO had a history of intervening on behalf of a weaker actor as evidenced by its military operations in Bosnia and Herzegovina in 1994 and in Yugoslavia in 1999, for example. While it couldn’t conclusively be determined that Russia was behind the cyber attacks, circumstantial evidence certainly pointed in its direction: some Russian computers being involved in the DDoS (as well as other countries in the world)[16], its perceived culpability in the instigating the riots in Tallinn, and the fact it made no overtures to stop or halt the attacks coming from its information space could have encouraged NATO to approach Russia. Diplomatic channels would invariably be exercised. Worst case scenario, diplomatic efforts would fail to achieve positive results, cooling relations between Russia and the Alliance. Therefore, when viewed as an instrument of policy, the DDoS attacks could be considered an unqualified failure that ran the risk of worsening formal relations or escalating into an international incident.

B. STUXNET – CYBERWARFARE HAS ARRIVED

Note: As of this writing, it is largely believed that the United States, and perhaps Israel, was involved in the creation and execution of Stuxnet. While unsubstantiated, this assertion gained additional legitimacy when an unidentified senior administration official “leaked” similar information[17]. If the U.S. government was behind the Stuxnet attack, the successful deployment of the weapon combined with the unofficial "leak" could have served an important U.S. foreign policy objective – to demonstrate to the Iranian government the complexities of U.S. capabilities and its ability to impact Iran's most sensitive programs.

In 2010, Iran publicly disclosed that a cyber weapon had damaged gas centrifuges in the uranium enrichment facility at Natanz. First identified by VirusBlokAda, Stuxnet was described as "highly sophisticated" and a 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.[18] The malware successfully impacted a significant number of Iranian centrifuges, targeting a specific type of industrial controller and causing almost 1,000 of them to spin out of control.[19] That malware had been injected into a network not connected to the Internet was nothing new. Individuals are constantly infecting stand-alone machines and networks via the witting or unwitting insertion of infected removal media. The significance of this event was the fact that this was the first documented incident where an actual cyber weapon was deployed whose intention was to deny, degrade, disrupt, and destroy a specific information system target. What's more, the sophistication of the malware, its functionality, the intent behind its deployment, and its clandestine appearance on a non-Internet connected industrial control system network pointed a finger squarely at nation state sponsorship, thus ushering in the first instance of cyberwarfare. Suspicions that the United States and Israel were the possible perpetrators of this act were bolstered but not confirmed in 2012 when an unnamed U.S. official acknowledged U.S. involvement as part of its classified "Olympic Games" program initiated by President George W. Bush and continued by President Barack Obama. The U.S. government has made no official pronouncement on the subject.[20]

1) Why Stuxnet?

It's little surprise that relations between the U.S. and post-Revolution Iran haven't been friendly. Iran's heated rhetoric, extremist religious views, and insistence on its sovereign right to develop nuclear power have caused the U.S. great concern over its intentions to use that capability to develop weapons grade uranium. Indeed, for the past few years, U.S. has closely monitored Iranian uranium development, and has even offered technological and economic incentives through international cooperation as a viable alternative to developing the capability indigenously and without regulatory oversight. Iran has consistently brushed aside these overtures, withstanding an onslaught of increasingly severe economic sanctions to affirm its right to nuclear self development.

If true, President Bush's decision to employ a cyber weapon of this caliber[21] was commendable in the fact that he saw this as a viable non-lethal option as opposed to approving a conventional military strike. Already embroiled in two military conflicts, the deployment of Stuxnet could have been intended to impede Iran's nuclear development without alerting them that this was the result of clandestine sabotage. For two years after its discovery, the U.S. remained tight-lipped about its role in Stuxnet despite international suspicions to the contrary. So if they were culpable, why would the U.S. publicly "leak" their involvement in Stuxnet in 2012? Some key events that transpired in the spring provide some illumination:

- March 14, 2012: In an interview with CNN, Iranian officials reiterate that nuclear inspectors would not be allowed to return.[22]
- March 5, 2012: Israeli President Benjamin Netanyahu travels to the United States and warns that a diplomatic solution to Iran's nuclear threat is running out.[23]
- March 3, 2012: U.S. President Barack Obama states that all elements of American power remain an option to prevent Iran from becoming a nuclear power.[24]
- February 24, 2012: The International Atomic Energy Association (IAEA) reports that Iran has significantly stepped up its uranium enrichment program and has concerns about potential military uses.[25]

These events show that over the course of 2012, Iran continually demonstrated its intentions to continue enriching uranium despite the European Union and United States economic sanctions and international disapproval levied against it. Therefore if the unknown U.S. official's admission of deploying Stuxnet is true, it can be interpreted as removing any doubt over U.S. involvement in trying to impede Iran's nuclear development. Not only would it have demonstrated the United States' sophisticated capabilities in the development of advanced cyber weaponry; but it also would have shown that it could "touch" Iran's most secret nuclear development facilities any time it wanted.

2) *But Did It Work?*

Aside from being a technological marvel at the time of its discovery, it is debatable if the deployment of Stuxnet achieved its true intended results. While U.S. officials might conclude the success of Stuxnet at "delaying" Iran's nuclear progression, it did not significantly impact Iran's plans or its ability to enrich uranium. On the contrary, the discovery of Stuxnet reaffirmed Iran's commitment to its nuclear program. While reports genuinely agreed that Stuxnet had effectively damaged 1,000 centrifuges in the Natanz facility, Iran had quickly recovered from the attack and replaced the effected centrifuges with new equipment, according to the Institute for Science and International Security, a Washington, D.C.-based non-partisan think tank.[26] Indeed, current evidence clearly indicates that Iran has actually stepped up its nuclear development capabilities. According to the *Washington Post,* the next IAEA report on Iran's nuclear facility is not due until mid-November 2012, but as of the end of October, Iran had added more than 600 centrifuges to its underground facility at Fordow.[27] Therefore, it is clearly evident that the cyber attack – while minutely slowing Iran's uranium enrichment – did nothing to dissuade it from pursuing its nuclear development objectives. Three truths emerged from this situation: 1.) Stuxnet did not cause Iran to alter its plans; 2.) The deployment of a cyber weapon did not influence the Iranian government to cease its production of enriched uranium; and 3.) Stuxnet did not encourage the government to come to an arrangement with the United States and European Union.

As a potential policy tool, the cyber attack achieved two unexpected consequences: it bolstered Iranian commitment to nuclear development as the government rapidly replaced all damaged centrifuges,[28] and it revealed that if the United States was responsible for the attack it would militarize cyberspace to pursue its objectives. Furthermore, revelation of Stuxnet has since compelled Iran to improve its cyber security posture through a series of government-led mandates and regulations. Perhaps of more concern, Stuxnet has allowed Iranians to study a tool that is designed to target and adversely impact an industrial control system. Given the increased concern expressed by U.S. policymakers and military decision makers of hostile actors targeting the United States supervisory control and data acquisition (SCADA) systems, an escalation over this nuclear issue could prompt Iran to use a similar type tool to "try to retaliate by attacking U.S. infrastructure such as power grid, trains, airlines, and refineries."[29]

Furthermore, evidence suggests that stringent sanctions are doing more to influence Iran into providing more transparency to its nuclear development, than Stuxnet or any subsequent malware discovery on Iranian networks. Since taking effect, sanctions have successfully weakened Iran's economy, causing inflation and deflating the value of the rial, Iran's national currency.[30] While this has not caused Iran to give up its plans for nuclear development, it has been instrumental in changing its views over the possibility of sitting down with the United States to discuss alternatives and possibilities. In November 2012, Iran's Ministry of Intelligence published a report on its website highlighting both Israeli and U.S. positions on Iran's nuclear aspirations with a favorable view of the U.S. desire to resolve the matter diplomatically rather than by military force.[31] Simply, multilateral economic sanctions and diplomatic overtures have had more influence to bringing this topic to a peaceful resolution. The cyber attack, on the other hand, did not dissuade Iranians.

C. *2012 DISTRIBUTED DENIAL OF SERVICE ATTACKS AGAINST U.S. FINANCIAL SECTOR*

Note: Although Iran has not claimed responsibility for this activity, it is assumed by U.S officials[32] that the government had at least an informal role in directing the distributed denial-of-service (DDoS) attacks against the U.S. financial sector. If the Iranian government was involved in directing or participating in the DDoS attack, and the activity was used as a foreign policy tool, then it can be interpreted as an Iranian effort to communicate to the United States that Iran had a formidable cyber capability, and to try to influence U.S. government courses of action toward the Islamic state.

From September-October 2012 an ongoing strategic DDoS campaign dubbed "Operation Ababil" was levied against several prominent institutions within the U.S. financial sector (Note: as of this writing, Phase 2 of Operation Ababil occurred in December 2012 and Phase 3 occurred in March 2013) . A self-described hacktivist group dubbed the "Cyber Fighters of Izz ad-Din Al Qassam," assumed credit for the attacks, claiming they were perpetrated in response to the anti-Islam film "Innocence of Muslims," which sparked worldwide controversy and physical protests. The targets of this sustained DDOS campaign were Bank of America, Wells Fargo, US Bank, JP Morgan Chase, Sun Trust, PNC Financial Services, Regions Financial, and Capital One. According to press reports, the attacks effectively cut bank customers off from online services for extended periods.[33]

1) *Who Are The Cyber Fighters of Izz ad-Din Al Qassam?*

Regardless of their public statements to the contrary, the Cyber Fighters of Izz ad-Din Al Qassam demonstrated little in common with traditional hacktivist groups such as Anonymous, LulzSec, or Anti-Sec. Additionally, while there have been instances of Islamic hackers unifying against a common foe (e.g., Israel during Operation Cast Lead), several facts suggest that this group was not composed of hacktivists at all but of more sophisticated individuals perhaps sponsored by or affiliated with a nation state. Several pieces of evidence support this line of thinking:

- Hacktivist groups typically target the subject of their ire; in this case, there were no cyber actions taken against Mark Basseley Youssef, the director of the controversial film, or anything related to him.
- There were no protest style cyber attacks directed against either Google or YouTube, the unwitting distributor of the film via its website. If the group believed Google to be complicit in posting the video, we could reasonably expect that the hacktivist group would have targeted Google. In this case, the Cyber Fighters of Izz ad-Din Al Qassam did not.

- The emergence of the Cyber Fighters of Izz ad-Din Al Qassam is suspect. While it's not uncommon for like minded individuals to quickly ban together under a common cause, there is no history of Islamic hacktivist groups demonstrating this type of capability. This group leveraged infections of high bandwidth servers as opposed to using participatory DDoS tools, which has generally been the case with Middle Eastern hacktivist groups. This suggests that these individuals had some affiliation with a nation state for training, technical support, and/or sponsorship.

The attackers used servers and customized malware, tailoring the campaign to get around defenses specifically designed to stop floods of data.[34] Given the technical savvy required to maintain a sustained DDOS attack against major financial networks, one would think that these individuals would be frequently engaged in Middle East disputes.

2) Mess With Us And We'll Mess With Your... Banks?

If cyber attacks are a possible government tool to support foreign policy objectives, two major questions need to be addressed in determining the utility of this new capability with respect to the 2012 DDoS campaign: (1) Why was the U.S. financial sector targeted with a sustained DDOS and (2) If the Iranian government had at least an informal role in directing the activity, did it achieve what it had set out to do?

U.S. officials and cyber experts have pondered the potential consequences of cyber attacks directed against the U.S. critical infrastructure and the damage it can cause due to the country's heavy reliance on computer networks and technology. In early 2012, President Obama identified cyber security as a national security priority alluding to the possible destruction of critical infrastructure networks as a real threat.[35] Indeed, even U.S. Secretary of Defense Leon Panetta warned of the possible ramifications of a cyber Pearl Harbor dismantling the nation's power grid, transportation system, and financial networks.[36] Suffice it to say, the U.S. Government has made it perfectly clear that it fears the possible consequences of such attacks against its well networked infrastructure.

Regardless of the motivations of the "alleged" hacktivist group behind the DDoS attacks, the targeting of the U.S. financial sector could be considered a retaliatory action for the Stuxnet incidents and U.S. sanctions levied against Iran for its continued nuclear development. For the former, Iran perceived the United States to be behind the cyber attack trying to destroy or at least disrupt the nuclear development process by infecting Iranian centrifuges.[37] For the latter, U.S. sanctions encouraged the Society for Worldwide Interbank Financial Telecommunication to block Iranian banks from using its service to conduct international banking transfers.[38]

Therefore, it can be argued that if Iran had some level of involvement in directing the DDoS activity, it was exercising a retaliatory strike.

The financial sector, as well as a nuclear industrial control system, is considered critical infrastructure, or networks essential for a functioning society. If the Government of Iran was involved in deploying the cyber weapon, they might have hoped to accomplish the following:

- Demonstrate its capability to target a critical infrastructure network using a technologically-based weapon instead of a more conventional one that would cause physical damage and potential loss of life;
- Retaliate with a measured response;
- Signal to the U. S. Government, as well as the region, that Iran has a cyber capability that can be deployed in a calculated manner against targets of its choosing.

While the attack did not cause any substantial damage to the targeted institutions, it did raise concern at the highest levels of the U.S. Government. Then U.S. Senator Joseph Lieberman in particular made public remarks attributing the activity to Tehran.[39] Although Iran never claimed official responsibility, it certainly made its intentions clear to the United States.

3) But Did It Work?

From an operational standpoint, the DDoS was an unqualified success. Banks were successfully targeted with a DDoS that took information sources offline or caused intermittent outages interrupting services. According to Prolexic Technologies, a company specializing in protecting organizations from DDoS attacks, sustained floods hitting 70 Gbps and more than 30 million packets per second were recorded in some of the attacks. When asked about the attacks, Dimitri Alperovitch, founder of CrowdStrike, said, "These banks… are not tiny. They have massive infrastructures…The fact that these attacks were able to shut down is quite remarkable." However, did Iran signal to the United States that it was a force to be reckoned with in cyberspace, perhaps a more subtle political objective of the government? Aside from signaling an Iranian cyber "show of strength," the DDoS attack failed to influence U.S. decision making or demonstrate to the U.S. government that Iran is a notable cyber force, based on the following:

- The United States did not alter its tough stance on Iran diplomatically nor did it repeal stringent economic sanctions levied against Iran.
- The United States withstood the most severe DDoS attack it has ever faced with relative ease without a prolonged hindrance to operations.

- Iran may have demonstrated the best it could do in a cyber attack capacity and the United States did not cower.

Therefore, the DDoS attacks did not prove to be a viable weapon of influence for the Iranian government if they were involved. It made no impact on U.S. plans and intentions toward Iran and its nuclear development, nor did it alter or amend its foreign policy positions. Viewing it from the narrow lens of foreign policy, the only conclusion that can be drawn was that the DDoS was a failure.

4. FUTURE CONSIDERATIONS

In October 2012, U.S. President Barack Obama signed a directive that enabled the military to act more aggressively against cyber attacks directed against the United States.[40] Lauded as a proactive step in countering the 21st Century's biggest threat, the new "policy" is intended as an equalizer to malicious online activity and a tool for military use. One U.S. defense official was quoted as saying, "cyberoperations… are an integral part of the coordinated national security effort that includes diplomatic, economic, and traditional military measures."[41] In short, the United States appears to be legalizing cyber attacks to be leveraged against those nations it perceives as a security threat without fully exploring the policy considerations that should accompany the deployment of cyber weapons as a policy tool.

Further complicating this scenario is how cyber weapons would be deployed against perceived nation state threats of varying cyber capability and/or information technology/Internet reliance. For a country like North Korea that has a near negligible Internet penetration rate, cyber attacks as a policy tool are almost futile. On the other end of the spectrum, take into account adversarial countries that have suspected and more robust cyber programs such as China and Russia. As one of the more wired countries in the world, and one whose officials routinely express concern about the security of its industrial control systems and critical infrastructures, is the United States prepared to potentially receive the same intensity of cyber attacks as it gives out? Finally, a third consideration addresses the identification of friendly and allied nations engaged in activities deemed a threat to national security such as the theft of sensitive and valuable military research and development, diplomatic, economic, and political information? Both France – a NATO member country – and Israel – the U.S.' strongest ally and a mutual defense treaty partner in the tumultuous Middle East region – have been identified as pervasive economic espionage actors against U.S. interests, according to the Central Intelligence Agency.[42][43] Would cyber attacks succeed in dissuading economic espionage, and is the cost-benefit worth the risk of breaking solid alliances.

5. CONCLUSION

Although the use of cyber attacks to support nation state foreign policy interests is still nascent at best, early indications clearly show it to be unsuccessful at influencing decision makers or their courses of action, and therefore is not an effective policy tool. Several factors account for this. First and most notably, despite the advanced cyber weaponry capabilities demonstrated by Stuxnet, Duqu, and Flame, there has yet to be that one "jaw dropping" effect that makes individuals think twice before booting up their laptops with malicious intent. Second, the threat of offensive cyber operations has a relative limited target base. For example, the threat of unleashing a sophisticated cyber weapon may carry more weight with a "wired" country like China or Russia than North Korea or even Iran, and has even less menace to nonstate actors that do not have a fixed infrastructure from which they operate. Finally, the deployment of cyber weaponry runs the risk of quickly and unnecessarily escalating a situation, particularly if cyber actions are misunderstood or misinterpreted by a clever adversary seeking to divert blame onto a third country.

REFERENCES

[1] John Brodkin; November 29, 2007; "Government-sponsored cyberattacks on the rise, McAfee says;"Network World; McAfee; http://www.networkworld.com/news/2007/112907-government-cyberattacks.html

[2] Ellen Nakashima, Greg Miller, and Julie Tate; June 19, 2012; "U.S. Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say;" The Washington Post; 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.

[3] The White House, International Strategy for Cyberspace; May 2011; http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[4] U.S. Department of Defense; July 2011; Department of Defense's Strategy for Operating in Cyberspace; http://www.defense.gov/news/d20110714cyber.pdf

[5] U.S. Department of Defense, Cyber Command Fact Sheet, 21 May 2010 http://www.stratcom.mil/factsheets/Cyber_Command/

[6] Gadi Evron, Winer/Spring 2008, "Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet War," Georgetown Journal of International Affairs, http://journal.georgetown.edu/wp-content/uploads/9.1-Evron.pdf

[7] Eneken Tikk, Kadri Kaska, and Liis Vihul, 2010, "International Cyber Incidents: Legal Considerations," Cooperative Cyber Defence Centre of Excellence, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

[8] William C. Ashmore; 2009; “Impact of Alleged Russian Cyber Attacks;” Baltic Security & Defence Review; Volume 11, 2009;

[9] Stephen Herzog; 2011; “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses; Journal of Strategic Study; Volume IV, Issue 2; pp.49-60.

[10] Peter Finn, May 9, 2007, “For Estonia’s Ethnic Russians, Ties to Moscow Fading,” Washington Post Online, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/08/AR2007050801935.html

[11] Irina Borogan and Andrewi Soldatov, April 25, 2012, “The Kremlin and the Hackers: Partners in Crime?” Open Democracy, http://www.opendemocracy.net/od-russia/irina-borogan-andrei-soldatov/kremlin-and-hackers-partners-in-crime

[12] Luke Harding; April 27, 2007; “Russia Up in Arms After Estonians Remove Statue of Soviet Soldier;” The Guardian; http://www.guardian.co.uk/world/2007/apr/28/russia.lukeharding/print

[13] Noah Shachtman; March 11, 2009; “Kremlin Kids: We Launched the Estonia Cyber War;” Wired.com; http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/

[14] Russian Law; March 6, 2009; “Russian Deputy Admits Involvement in Cyber Attacks on Estonia;” Russian Law Online; http://russian-law.livejournal.com/24179.html

[15] Joshua Davis; August 21, 2007; “Hackers Take Down Most Wired Country in Europe;” Wired Magazine; http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all

[16] Europe Edition; May 10, 2007; “A Cyber Riot;” The Economist Online; http://www.economist.com/node/9163598

[17] David E. Sanger, June 1, 2012, “Obama Order Sped Up Wave of Cyber Attacks Against Iran,” New York Times, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0

[18] Matthew Schwartz, June 1, 2012, “Stuxnet Launched by United States and Israel,” Information Week, http://www.reuters.com/article/2011/12/02/us-cyberattack-iran-idUSTRE7B10AV20111202

[19] Ellen Nakashima, Greg Miller, Julie Tate; June 19, 2012; “U.S. Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say;” The Washington Post; 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.

[20] David E. Sanger, June 1, 2012, “Obama Order Sped Up Wave of Cyber Attacks Against Iran,” New York Times, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0

[21] David E. Sanger, June 1, 2012, “Obama Order Sped Up Wave of Cyber Attacks Against Iran,” New York Times, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0

[22] CNN Wire Staff; March 19, 2012; “Timeline of Iran’s Controversial Nuclear Program;” CNN.com; http://www.cnn.com/2012/03/06/world/meast/iran-timeline/index.html.

[23] CNN Wire Staff; March 19, 2012; "Timeline of Iran's Controversial Nuclear Program;" CNN.com; http://www.cnn.com/2012/03/06/world/meast/iran-timeline/index.html.

[24] CNN Wire Staff; March 19, 2012; "Timeline of Iran's Controversial Nuclear Program;" CNN.com; http://www.cnn.com/2012/03/06/world/meast/iran-timeline/index.html.

[25] CNN Wire Staff; March 19, 2012; "Timeline of Iran's Controversial Nuclear Program;" CNN.com; http://www.cnn.com/2012/03/06/world/meast/iran-timeline/index.html.

[26] Joby Warrick; February 16, 2011; "Iran's Nuclear Natanz Facility Recovered Quickly From Stuxnet Cyber Attack;" The Washington Post Online; http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html

[27] Walter Pincus; November 1, 2012; "All Politics Are Local In Iran Nuclear Dispute;" The Washington Post; http://articles.washingtonpost.com/2012-10-31/world/35501296_1_nuclear-facilities-iaea-report-nuclear-program

[28] Mark Clayton, January 3, 2011, "Stuxnet Attack on Iran Nuclear Program Came About A Year Ago, Report Says," Christian Science Monitor, http://www.csmonitor.com/USA/2011/0103/Stuxnet-attack-on-Iran-nuclear-program-came-about-a-year-ago-report-says

[29] Brian Ross; March 5, 2012; "What Happens to the U.S. If Israel Attacks Iran?:" ABC News online; http://abcnews.go.com/Blotter/israel-attacks-iran-gas-prices-cyberwar-terror-threat/story?id=15848522#.UJqwOIZCjZ4

[30] Glenn Greenwald, October 7, 2012, "Iran Sanctions Now Causing Food Insecurity and Mass Suffering," The Guardian, http://www.guardian.co.uk/commentisfree/2012/oct/07/iran-santions-suffering

[31] Jason Rezaian, November 7, 2012, "Iran Ministry Suggests Openness to Nuclear Talks," The Washington Post, http://articles.washingtonpost.com/2012-11-07/world/35504040_1_nuclear-program-nuclear-talks-nuclear-facilities

[32] Ellen Nakashima, September 21, 2012, "Iran Blamed for Cyber Attacks on US Banks and Companies," The Washington Post, http://articles.washingtonpost.com/2012-09-21/world/35497878_1_web-sites-quds-force-cyberattacks

[33] Ellen Messmer; October 24, 2012; "DDoS Attacks Against Banks Raise Question: Is this Cyber War?" Network World online; http://www.networkworld.com/news/2012/102412-bank-attacks-cyberwar-263664.html

[34] Robert Lemos; October 4, 2012; "Serious Attackers Paired with Online Mob in Bank Attacks;" Dark Reading Online; http://www.darkreading.com/advanced-threats/167901091/security/perimeter-security/240008534/serious-attackers-paired-with-online-mob-in-bank-attacks.html

[35] Manuel Flores; July 25, 2012; "Obama Makes Cybersecurity a Priority;" Independent Voters Network Online; http://ivn.us/2012/07/25/obama-makes-cybersecurity-a-priority/

[36] Elizabeth Bumiller; October 11, 2012; "Panetta Warns of Dire Cyber Attack on U.S.;" The New York Times Online; http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all

[37] Associated Press, April 16, 2011, "Iran Blames U.S., Israel for Stuxnet Malware," CBS News, http://www.cbsnews.com/2100-202_162-20054574.html

[38] Don Melvin and Jonathan Fahey; March 15, 2012; "SWIFT Cuts Off as Sanctions Vice Tightens; "The Huffington Post; http://www.huffingtonpost.com/2012/03/15/swift-iran-sanctions_n_1347361.html

[39] David Goldman; September 28, 2012; "Major Banks Hit With the Biggest Cyber Attack in History;" CNN.com; http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html

[40] Ellen Nakashima; November 14, 2012; "Obama Signs Secret Directive to Help Thwart Cyberattacks;" Washington Post Online; http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html

[41] Ellen Nakashima; November 14, 2012; "Obama Signs Secret Directive to Help Thwart Cyberattacks;" Washington Post Online; http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html

[42] From Reuters; August 15, 1996; "France, Israel Cited in CIA Espionage Study;" Los Angeles Times Online; http://articles.latimes.com/print/1996-08-15/business/fi-34524_1_economic-espionage

[43] John A. Nolan; October 2000; "A Case Study on French Espionage: Renaissance Software;" http://www.hanford.gov/files.cfm/frenchesp.pdf