Confluence INVESTMENT MANAGEMENT

Weekly
Geopolitical Report

By Kaisa Stucke

June 22, 2015

Cyber Security and Terrorism: Case Studies

In April 2007, Estonian government workers found their internet connectivity interrupted and e-mail access compromised. In hindsight, this marked the beginning of a three-week cyber attack on the country's government and private servers. The attacks forced many servers to block international connections. At the same time, street riots by ethnic Russians were erupting in the country in response to the Estonian government's decision to move a war memorial for fallen Soviet soldiers from the center of the capital to a military cemetery. It is still unclear who was actually responsible for the cyber attacks, but these events are considered to be the first cyber attacks aimed at a sovereign nation, and were significant in setting a precedent for future cyber incidents.

In August 2008, the country of Georgia experienced multi-faceted cyber attacks targeted at government websites. The country's servers were overloaded with connection requests coming from abroad, forcing many servers to go offline. Additionally, many government websites were defaced with images of various fascist leaders. Concurrently, Georgia and Russia were involved in a military conflict in South Ossetia, in the northern regions of Georgia. It is also still unclear who was responsible for these attacks, but this is considered to be the second large-scale organized attack against a sovereign nation.

Sometime in June 2010, the Stuxnet computer malware started striking industrial facilities across Asia and the Middle East, with 60% of the affected computers residing in Iran. The most notorious of the attacks was targeted at the Bushehr nuclear facility in Iran. The Stuxnet malware was created to specifically attack industrial applications and was very complex in its mechanics and in avoiding detection. Again, no group has claimed responsibility and it is still unclear who was responsible for the attacks. This malware was very sophisticated, thus leading many observers to speculate that a private entity would not have had the resources to create it, suggesting that a nation state could have been responsible. Some observers call the Stuxnet virus the first cyber weapon.

This week we will look at these two case studies of cyber attacks aimed at sovereign nations. We will not cover the Stuxnet virus in detail in this report as we have written about it in the past.[1] We will then look at the current state of international cyber attack research, readiness and cooperation. We have had the pleasure of talking to the NATO Cooperative Cyber Defence Center of Excellence about their work and will communicate their vision and challenges.

[1] See WGR, 10/4/2010, The Stuxnet Virus.

Estonia 2007

On Friday, April 27, 2007, Estonian government officials were not able to log onto their e-mail in what they thought was a regular internet interruption. Although government connectivity and other political and commercial sites experienced difficulties, nobody suspected a wide-scale attack. Workers left for the weekend expecting technical issues to be resolved by Monday. On Friday evening, the defense minister suspected that all was not well when he attempted to log onto his account at the Estonia Reform Party's server. The Reform Party's website was the first to be attacked, but all parties' sites were eventually targeted. This was the beginning of a three-week cyber attack on the country.

The cyber attacks came in the form of a flood of "ping" requests to servers, overwhelming the servers' ability to process the requests. During normal server interaction, servers communicate with each other by sending pings from server one to server two; in turn, server two sends a ping back to confirm connectivity. Under normal circumstances, this happens seamlessly and does not slow the connection. The attacks on Estonia used the same process, only they employed a huge number of ping requests. According to estimates, at its height, some servers in Estonia received 4 million pings per second, leading to slowness and failure. It would be similar to 4 million individuals per second trying to connect to the same website at once. Although the mechanics of the attack itself are not necessarily complicated, the number of pings produced made it an effective weapon, which is extremely hard to track due to the short-term nature of the communication. Additionally, hackers can use servers and computers that are domiciled in various countries, making it much harder to track their footprints. Reportedly, up to 50 countries' servers were involved in the attacks.

Some experts call the 2007 Estonian cyber events "cyber riots" rather than "cyber war." The attacks were widespread, and aimed at creating confusion and demonstrating the ability of the outside power to take control of the country's cyber-sphere. In order to repair the server damage, the government and some private news agencies had to resort to blocking international pings. In practical terms, this blocked all international access to these websites. Ironically, the news agencies' ability to communicate the cyber attack development in Estonia were hindered, leaving outside observers speculating about the degree of damage.

The attacks were entirely unexpected and Estonia lacked the necessary technical capabilities to protect itself from cyber attacks. The country has built an impressive technological network. Reportedly, 60% of the population relies on the internet for critical tasks on a daily basis. About 96% of bank transactions are done over the internet. Voting can be done over the internet as can paying taxes. Estonia relies heavily on the internet for critical functions and this reliability on the cyber services created a unique vulnerability. Also, the rapid pace of cyber development had far outpaced the development of defensive measures.

The origin of the attacks is still unclear and no party has stepped forward to claim responsibility. Some observers have pointed to Russia as the most likely culprit. The Russian Duma has denied its involvement, but some Russian activists have suggested that rogue hackers connected to the youth political movement, Nashi, were behind the attacks. The cyber landscape allows for a small group of hackers to wreak havoc, so it

is possible that an independent group of hackers caused the attacks.

Without knowing the originator of the attacks, we are left guessing their motivation. Outside of the cyber world, the relationship between Estonia and Russia had become quite hostile. The government of Estonia had decided to move a memorial to fallen Soviet soldiers from the center of the capital to a military cemetery. To Estonians, the memorial was a reminder of the Soviet occupation, while for Russians, it served as a memento for their lost soldiers. The decision to move the memorial resulted in ethnic Russian-led street riots in Estonia and trade sanctions imposed by Russia. However, this is just one instance of a very complicated relationship. With this background it would seem reasonable to suspect that the cyber attacks originated from hackers in Russia.

The significance of the Estonian cyber attacks lies not in the size or scope of the attacks, but the precedent that it set for future cyber conflicts. Cyber defense has been a political priority for NATO for decades, but the Estonian incidents reinforced the need for a NATO-wide strategy. In 2008, NATO established a cyber defense center, which is located in Estonia.

Georgia 2008

The second known cyber attack on a sovereign nation occurred on August 8, 2008, in Georgia. Again, government servers were overwhelmed by the number of ping requests. Additionally, many government websites were hacked and information was changed. At one point, the Ministry of Foreign Affairs website had a picture of Georgian President Mikhail Saakashvili next to an image of Adolf Hitler. The country was taken by surprise by the cyber attacks and had little time to react. Hoping to engage international forces, the Georgian government moved President Saakashvili's website hosting to a server located in Atlanta, Georgia.

According to experts, the Georgian incident was the first time that a cyber attack coincided with conventional warfare. The relationship between Georgia and Russia had been complicated ever since the fall of the Soviet Union. Two northern regions of Georgia, South Ossetia and Abkhazia, declared independence and were generally aligned with Russia. Civilian hostilities intensified between South Ossetia and Georgia in 2008, which resulted in large-scale armed conflicts in the region and Russian military moving into the region.

Although the Georgian government has blamed the Russian government for the attacks, it is still unclear who was responsible. Again, as was the case with the Estonian attacks, it is possible that an independent group of hackers targeted Georgian servers. There is some evidence to believe that the Russian government was not directly responsible for the attacks. The attacks sought to intimidate and interrupt the flow of government information, but did not target the country's infrastructure. If Russia wanted to, it could have easily disrupted oil flows through cyber attacks, causing severe financial damage for Georgia. However, none of the infrastructure was targeted. On the other hand, there is evidence that if the government was not directly involved, it could have shared information with the hackers. For example, the conventional and cyber attacks were both targeted at the same cities at the same time. The Russian government denies its involvement.

Cyber War vs. Cyber Crime
Generally speaking, cyber attacks are any action taken to disrupt, deny, degrade or destroy information on a single computer or a computer network.

It is important to differentiate between organized cyber crime and cyber war. Organized cyber crime's goal is financial gain for the hacker, either directly through illegally transferring funds or by turning the victim's computer into a "zombie machine," which is then used in other cyber attacks. On the other hand, cyber war's main goal is to gain control and intimidate the target, with the target being a sovereign country's public or private information system. Cyber terrorism is defined as the politically motivated use of computers and information technology to cause severe disruption or widespread fear.

Cyber attacks allow for small groups to have a disproportionate ability to cause damage on a large scale as even a single skilled hacker could cause serious damage. Additionally, cyber attacks are so inexpensive and hard to track that they're likely to be used frequently, either in conjunction with conventional warfare or independently. Organizing a cyber attack is becoming increasingly easier as hackers often share corrupted codes over internet chat rooms.

NATO Capabilities and Cooperation
The NATO Cooperative Cyber Defence Centre of Excellence is based in Tallinn, Estonia, and serves as the main source of expertise in the field of cooperative cyber defense within NATO. The center's mission is to enhance the capability, cooperation and information sharing among NATO, its member countries and partners. We note that the center itself does not provide cyber defense to member countries. The center is only responsible for its own network's cyber security, while each member country is responsible for its own defense.

We had the pleasure of talking to the center about its priorities and thinking around cyber defense. The following is a combination of our own research as well as thoughts shared by NATO.

Thus far, no country has declared a cyber war; in fact, cyber attacks go unnoticed for days, weeks and months. Additionally, there will be very few footprints left behind from successful cyber aggression. The complex network used by cyber terrorists will make attribution complicated and challenging. However, with advancing technologies and the integrated nature of modern nation states, cyber warfare is likely to become an increasingly important part of the political and military arsenal.

Currently, a coordinated international response is somewhat difficult as each NATO country has developed its own cyber defense systems. Even the definitions used in communicating cyber defense differ between countries. For example, there are no less than ten definitions for the term "cyber attack" among the member countries. Integrating the national networks will prove to be complicated and the changing nature of cyber threats will continue to challenge both NATO and each of its member countries independently. Furthermore, given the international nature of cyber attacks, the legal implications are complicated.

In 2007, a NATO official asked, "If a member state's communications center is attacked with a missile, you call it an act of war. So what do you call it if the same installation is disabled with a cyber-

attack?"[2] The general answer seems to be, "you still call it an act of war," but the responsibility to discover the cyber attack and find the culprit falls on each country.

Ramifications

Cyber attacks are likely to become an increasing part of international aggression, either used independently of or in conjunction with conventional warfare. The attacks are also likely to grow in sophistication, with many of them never getting detected.

The ability of small and independent groups to cause disproportionately large amounts of damage will move power from the nation states to NGOs. Smaller NGOs have the ability to both organize cyber attacks and respond to them more efficiently.

Kaisa Stucke
June 22, 2015

[2] A Cyber-Riot. (2007, May 10). *The Economist*.