Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective

Rain Ottis
Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia
firstname.lastname@mil.ee

Abstract: Following the relocation of a Soviet-era statue in Tallinn in April of 2007, Estonia fell under a politically motivated cyber attack campaign lasting twenty-two days. Perhaps the best known attacks were distributed denial of service attacks, resulting in temporary degradation or loss of service on many commercial and government servers. While most of the attacks targeted non-critical services like public websites and e-mail, others concentrated on more vital targets, such as online banking and DNS. At the time of this writing – more than six months after the cyber attacks – no organization or group has claimed responsibility for the cyber attacks, although some individuals have been linked with carrying them out.

This paper will argue that the key to understanding the cyber attacks that took place against Estonia in 2007 lies with the analysis of an abundance of circumstantial evidence that ran parallel to the cyber attacks. These consisted of political, economic and information attacks on Estonia, as well as isolated cases of physical violence. Clear political signatures were even detected in the malicious network traffic. All told, it is clear that the cyber attacks were linked with the overall political conflict between Estonia and Russia.

While some analysts have considered last year's events in Estonia an international, grass roots, display of public opinion, there are some direct and many indirect indications of state support behind what can be best described as an information operation. By information operation, the author means the use of information and information technology to affect the decisions and actions of an opponent.

The paper will give an overview of the major events and provide an analysis of the attacks from the information warfare perspective. The paper will also discuss some of the potential problems with using the Internet as a field of battle by lone hackers, terrorist groups and states. To a minor degree, the paper will also cover the difficulties associated with investigating and analyzing international cyber attacks. The objective of this paper is not to implicate a specific organization or entity, but to provide a wider view to the cyber attacks that were carried out against Estonia in the spring of 2007.

Keywords: cyber attack, information operation, people's war

1. Introduction

In the spring of 2007 Estonia fell under a cyber attack campaign lasting a total of 22 days. The attacks were part of a wider political conflict between Estonia and Russia over the relocation of a Soviet-era monument in Tallinn. Due to the lack of definitive quantitative data, the author will use qualitative analysis to explain the cyber attacks.

1.1 The trigger

The trigger for the event was the Estonian government's decision to relocate a monument to Soviet troops from a busy intersection in central Tallinn to a nearby military cemetery. The monument depicting a Soviet soldier was originally erected in 1947 at the burial site of Soviet troops who died while taking Tallinn in World War II. Since that time the monument has developed two very distinct identities. For the local Russian minority it represents the "liberator" while for the Estonians it represents the "oppressor".

Over the past few years the statue had become a focal point of tension between pro-Kremlin and Estonian nationalist movements. In order to defuse the situation and to relocate the war-dead from a traffic intersection to a more peaceful resting place the Estonian government decided to move the monument and the accompanying remains to a military cemetery in Tallinn. Work began on the 26th of April 2007. During the day, mostly peaceful protesters gathered at the site, but in the evening a more violent crowd emerged. After a few hours of violent clashes with the police the rioters turned away and proceeded to vandalize and loot the nearby stores. Police regained control of the situation by morning.

However, the 27th of April marked the beginning of cyber attacks that targeted Estonian internet-facing information systems. Attacks of various types continued for a total of 22 days. Even though the attack types were well known, they were unparalleled in size and variety compared to a country the size of Estonia. Furthermore, Estonia is highly networked, so a wide scale attack on the availability of public digital services has a significant effect on the way of life of ordinary citizens and businesses alike. Therefore, these cyber attacks can not be disregarded as mere annoyances but should be considered a threat to national security.

1.2 Overview of associated events

During the 27th of April there were several smaller standoffs between rioters and police. Throughout this time, both local and international media reported on the street riots. Interestingly, the looting of the stores and destruction of property was not covered by Russian media, who mostly reported on police violence against "peaceful protesters". This fueled an array of angry articles and statements from Russia, including a statement by a member of the Russian parliament that this event should be cause for war (ICDS 2007). It is therefore understandable why many Russians could be inclined to participate in various actions against Estonia.

Aside from the cyber attacks, the most notable events transpired at the Estonian embassy in Moscow. Pro-Kremlin youth groups staged well organized and equipped protests for many days and at times actually prevented Estonian embassy workers and diplomats from entering or exiting the building. The climax came on May 2nd, when the Estonian ambassador was physically attacked during a press conference. (ICDS 2007)

Another aspect of the conflict was economical. While officially no economic sanctions were imposed on Estonia by Russian authorities, the trade relations deteriorated. Many companies in Estonia lost revenue with Russian trade. This could be explained as a patriotic reaction by the business owners in Russia. On the other hand, the sudden ban on heavy commercial truck traffic at a border bridge in Narva clearly required Russian government involvement (Ottis 2007). The ban was lifted when the situation calmed down.

2. Facts

For this analysis, the author was able to re-use facts gathered for an earlier analysis of the same event (Ottis 2007). In addition, updated information from the Estonian State Procurature is included.

2.1 Facts collected by the author during and after the events in question

- The cyber attacks in question took place between 27 April and 18 May of 2007. The focus, method and volume of the attacks shifted during this period, but most of the detected attacks can be attributed to the same underlying event.
- The vast majority of the malicious traffic originated from outside Estonia. To combat this, some banks temporarily cut off all foreign traffic while remaining accessible for clients in Estonia. This white list was then gradually expanded to include the countries with many clients but few attackers.
- The malicious traffic often contained clear indications of political motivation and a clear indication of Russian language background. For example, malformed queries directed at a government website included phrases like "*ANSIP_PIDOR=FASCIST"* (Mr. Ansip was the Estonian Prime Minister at the time). Dozens of variants were used, often containing profanities.
- Instructions for attacking Estonian sites were disseminated in many Russian language forums and websites. These instructions often included motivation, targeting and timing information, as well as a specific description for launching attacks. An example of these instructions is displayed in Figure 1. Note that this excerpt includes information about when, what and how to attack. It also illustrates how simple the most primitive attacks are to organize, provided you can motivate enough people to execute these simple instructions. With thousands attacking, even a primitive ping flood can cause trouble.

Figure 1: An excerpt of the attack instructions found on a web site during the event.

- In general, the attacks can be described as Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks. Many well known methods were used, including ping flood, udp flood, malformed web queries, e-mail spam, etc.
- A few more complex attempts were made to hack into systems, for example using SQL injection. Some of these attacks met with success at non-critical sites.
- The targeted systems included web servers, e-mail servers, DNS servers and routers. Most visible to the public were the attacks against web servers.
- The targeted entities included the government, the president, the parliament, police, banks, Internet service providers (ISPs), online media, as well as many small businesses and local government sites.
- May 9th is an important date in this event, because that is when Russians celebrate victory over Nazi Germany. On many sites (including the example in Figure 1) the organizers called for an attack on that politically important date. The big attack wave anticipated for May 9th started shortly after 11PM local time on May 8th, however, suggesting that these attackers were on Moscow time.

2.2 Facts gained from the Estonian State Procurature in January 2008

- As of January 2008, only one person has been convicted of carrying out cyber attacks in the spring of 2007. Dmitri Galuškevitš, a 20-year old student in Estonia was fined for organizing a DDoS attack against the website of a political party in Estonia. His conviction was possible because he committed the attacks from Estonia and therefore enough evidence could be collected.
- The Estonian State Procurature made “a formal investigation assistance request” to the Russian Supreme Procurature in May of 2007, in order to track down attackers residing in Russia. As of January 2008, this has not yielded any positive response, regardless of the fact that this type of cooperation is specifically “enumerated in the Mutual Legal Assistance Treaty” between Estonia and Russia.

3. Analysis

The analysis will attempt to find a plausible explanation for the cyber attacks that took place against Estonian information systems between 27th of April and 18th of May 2007. Due to the nature of the facts gathered in the previous chapter, the author will use qualitative analysis. Several hypotheses are considered:

- The event was a Russian information operation against Estonia
- The event was a false flag operation to frame Russia as the attacker
- The event was a spontaneous grass root level response to the policy of the Estonian government

This is not a complete listing, but the author feels that these three can be considered as the most probable explanations to the event.

3.1 Information operation

In this analysis, the author considers an information operation as the use of information and information technology to affect the decisions and actions of an opponent. In an article about possible Chinese strategies for invading Taiwan, Wu (2004) points out the possibility of using the information age equivalent of the concept of *people's war*. In the context of cyber attacks, this means that ordinary citizens of a state can be motivated to use the resources under their control to independently attack enemy systems in order to confuse the defenders. Amidst all the noisy and ill-coordinated attacks, more professional intrusions can then be carried out, supplemented with physical attacks to take out the command and control systems of the opponent. (Wu 2004) The beauty of people's war is that it provides near perfect deniability for the government or any other entity that is behind the attacks.

In order to consider this hypothesis plausible in the context of people's war, we need to show that:

- many people of varying skill levels took part in the attacks;
- the people who committed the attacks were externally motivated; and,
- the attackers received some form of support from the state.

Judging from the variety and volume of different attacks, it is likely that they were committed by many different individuals. The only person convicted of taking part in the attacks was shown to be responsible for an insignificant fraction of the attacks while further investigations have stagnated due to the lack of cooperation by Russian authorities. The activity in forums at the time of the attacks also indicates widespread interest in attacking Estonia. The attacks ranged from manually launching pings to botnet DDoS's to exploiting specific vulnerabilities in router software. Many of the detected attacks were described in detail on various Russian language forums and websites, which were easily available to those interested in finding a way to participate in the attacks. Most of these instructions were extremely simple to execute, thus making the prior experience of the attackers irrelevant. Therefore, we can say that many people of varying skill levels likely took part in the attacks.

It is also clear that the attacks were politically motivated because many of them contained a message related to the overall conflict surrounding the statue. The hostile rhetoric from various high ranking politicians in Russia were broadcast in the media and disseminated further in forums and web portals. On some of these forums there were open discussions about attacking Estonian systems or collecting resources for renting botnets. Taking the preceding factors into consideration, one can easily see that the attackers received encouragement from high ranking members of the Russian political elite.

The Russian government has consistently denied any direct involvement in the cyber attacks that hit Estonia in the spring of 2007. To the author's knowledge this claim is true. It is remarkable, however, that neither is there any proof of measures taken by the Russian government to mitigate the situation. The lack of cooperation in the Estonian investigation indicates that the Russian government is not interested in identifying the attackers and is therefore, in essence, protecting them. In other words, hostile rhetoric from the political elite motivated people to attack Estonia while nothing was done to stop the attacks. This silent consent, however, can be interpreted as implicit state support because without fear of retribution the attackers were free to target Estonian systems.

Assuming that this event was a result of a deliberate information operation, it is most likely tied with the larger political conflict that surrounded it. Since no entity has claimed responsibility for organizing the attacks, the author can only speculate as to the aim of this operation. In this case, the aim could be to unite the Russian people against a common enemy before the elections. Another possibility is to

destabilize the Estonian society and to undermine the Estonian economy in an effort to weaken its ties to the European Union and the North Atlantic Treaty Organization. Yet another is a proof of concept on the digital people's war idea while supporting the overall political campaign surrounding the statue. At least in theory, several reasons can be found for conducting this type of operation.

If the cyber attacks were the result of an information operation, then one could argue that it was fairly effective. Large scale attacks were mounted against an independent state while no controlling entity (government or otherwise) has been identified. This would be an invaluable lesson for preparing for future conflicts. Therefore, this hypothesis can be considered plausible.

3.2 False flag operation

It has been suggested that the cyber attacks could have been a false flag operation. In other words, that the theoretical mastermind behind the attacks wanted to make it look like it was originating from Russia. While an interesting theory, it fails to explain the hostile statements of the Russian officials and the complete lack of cooperation on the investigations of the cyber attacks originating from Russia. In case of a false flag operation, it would be in Russia's interest to show the world that they were in fact not behind the attacks and better yet, to expose the entity that planned it. As a result, this hypothesis is implausible.

3.3 Grass roots response

Another theory is that the cyber attacks were nothing more than a wide scale, international, grass roots protest against the policies of the Estonian government. This would explain why no organization, agency or government has taken responsibility for the attacks. Unfortunately, this theory would require only spontaneous actions of the people while silent state support has already been demonstrated in previous sections. Once we admit the state as one of the partners in the protest, it is no longer grass roots or independent. Therefore, this hypothesis is implausible.

4. Lessons learned

One of the biggest lessons emerging from this event is that in a modern conflict, cyber attacks are becoming increasingly more common and dangerous. Any country with sufficiently well developed network infrastructure is vulnerable to these attacks. Primitive cyber attacks take very little time and effort to organize, while defending against them is becoming more and more difficult. Under the cover of the primitive and noisy attacks, more professional intrusions can be performed to gain a foothold for further attacks.

There are several problems with using the Internet as a field of battle by lone hackers, terrorist groups and states. First, the Internet spans the globe, thus a large scale attack is likely to influence innocent bystanders in other countries as well as the target country. Therefore, some of these attacks could be classified as terrorist activity, since they target civilian systems in the hopes of getting more attention from the press.

Second, the relative anonymity of the Internet allows for a near perfect deniability, as was the case in Estonia. All one has to do is either originate the attack from or route the traffic through a country that is not willing to cooperate. This makes it almost impossible to bring the attackers to justice, especially when considering the lack of common international legal grounds for these new types of attacks and conflicts.

Third, a new phenomenon is currently emerging that could change the concept of information assurance in a radical fashion. This phenomenon is the militarization of cyber space. Most systems today are built with lone hackers and script kiddies in mind. But militaries are moving into cyber space. What if all the nationally critical systems fall under a simultaneous concentrated cyber attack from thousands of professional, well trained and equipped cyber attackers? In a war scenario, these attacks would most likely be complemented with physical destruction at some key sites, as well as special operations troops capturing others. The author believes that this could be devastating to any country with a developed network infrastructure. Organized military resistance could be knocked out overnight, in theory.

5. Summary

The analysis of the cyber attacks that hit Estonian systems in the spring of 2007 is a difficult task due to the fact that a large part of malicious network traffic data is unobtainable. This, in turn, does not allow the investigators to pursue many of the people who committed the attacks. Therefore, the author used qualitative analysis of the known facts to provide an overall explanation for the event.

Of the three hypotheses considered, only one was determined plausible. The author concluded that the event can be explained as a Russian information operation against Estonia. Specifically, this event seems to match the digital version of the Chinese concept of people's war, where the government motivates people to attack its enemies by any means at their disposal. The digital version provides plausible deniability for the government, while in the case of this event the government can easily protect the attackers by refusing to cooperate with foreign investigators. This scenario illustrates the many dangers that come with using the Internet as a battle space.

It should be noted that this analysis does not *prove* that there was an information operation due to lack of evidence from the Russian authorities. Instead, the conclusion is considered *plausible* and in line with the available facts. If the Russian authorities were to release the necessary technical evidence, a more thorough quantitative analysis could be conducted, which could lead to the attackers.

References

International Centre for Defence Studies (ICDS) (2007) "Moskva käsi Tallinna rahutustes. Rahvusvahelise kaitseuuringute keskuse kiirülevaade 7. mail", *Sõdur*, No 2, pp 4-8. *(Moscow's Hand in the Tallinn Riots. A Quick Overview by the International Centre for Defence Studies on 7th of May)*

Ottis, R. (2007) *Analysis of the Attacker Profiles in the 2007 Cyber Attacks Against Estonia*. Unpublished MSc dissertation, Tallinn Technical University, Tallinn.

Wu, C. (2004) "An Overview of the Research and Development of Information Warfare in China." In Edward Halpin et al (eds.) (2006) *Cyberwar, Netwar and the Revolution in Military Affairs*. Palgrave MacMillan, Hampshire, pp 173-195.