"Cyber warfare", the truth in a real case

Muhammad Saleem Jawad Hassan
Email: {muhsa378, jawha562} @student.liu.se
Supervisor: Viiveke Fåk, {viiveke@isy.liu.se }
Project Report for Information Security Course
Linköping Universitetet, Sweden.

Abstract

Attacks against IT systems are common and attackers are often making headlines by compromising secure and critical systems to carry out malicious activities. These attacks aggravate during political conflicts and hackers get involved in destroying each other's IT infrastructure ultimately leading to a cyber war. History has witnessed many cyber wars and the cyber attack against Estonia in April 2007 is one of the recent examples of such conflicts, which brought another dimension of war in information age. This paper will cover in detail the cyber attacks against Estonia and will highlight many issues associated as a result from this conflict. This paper will also cover the tools and techniques used to carry out the attacks against Estonia along with possible defences and tracing of the perpetrators.

1. Introduction

IT systems are increasingly networked to take competitive advantage in information age, in an effort to provide better customer facilities i.e. E-commerce, instant access to information, etc. Networking of critical systems exposes them to a large pool of attackers who exploit vulnerabilities in non-secure systems – severely effecting normal business processes with malicious activities. A number of cyber wars have been reported in recent history briefly outlined here. In 1999, the cyber war between Pakistan and India started when armed forces of both the countries were engaged on the battlegrounds of Kargil. In 2003, the US servers were under attack by hackers alleged to be of Chinese origin in order to reveal US government secrets [1]. In April 2007, Estonia's IT infrastructure came under heavy attack by Russian hackers, damaging critical Estonian websites and servers [2]. In December 2007, large number of Kyrgyz websites came under heavy attack during the election campaign [3]. In October 2008, Russia launched a cyber attack along with a conventional attack on critical Georgian websites and servers disabling their communication and information services [4].

This paper will cover important dimensions of the Russian and Estonian cyber conflict that severely damaged Estonian's IT infrastructure. First, we will go through the prime reasons of this conflict and how it ultimately leads to this disastrous event. In section 2 (attack on Estonia's IT infrastructure), we will cover the impact of the attack, damages caused by the attack, facts and figures, tools and techniques used to carry out the attacks, types of attacks, and possible defences to safeguard IT systems against such attacks in future. Section 3 (news reports and expert views) will cover reports published by famous newspapers and its impact on the normal news readers. Section 3 will also cover expert views on those attacks. Conclusion will be drawn in section 4 based on our research. Finally, references will be provided for further reading on this issue.

2. Attack on Estonia's IT infrastructure

In April 2007, differences between Russia and Estonia surfaced, when Estonia relocated the bronze soldier of Tallinn, a soviet-era war monument from the centre of Tallinn – which resulted in a strong protest among Estonians of Russian descent who considered this monument as a symbol of honour to the Red army who fought against German Nazis. However, Estonian's viewed the monument as a symbol of foreign occupation and used to protest every year for its removal from Tallinn. During protest by Estonian's of Russian origin, who viewed statue as a symbol of their right to be in

Estonia, around 1300 people were arrested, 150 were injured, and one person killed. This incident also raged anger all across Russia and Russian computer experts turned to computer to attack Estonian's IT infrastructure. This was a major blow since Estonia was heavily dependent on IT services. Thus started the fifth dimension of 'cyber wars' besides the conventional mediums of air, ground, sea and space wars [5]. Estonia implicated the Russian government for the attacks but Kremlin denied any type of involvement.

2.1. Impact of Attack

Estonia, the country with a population of 1.4 million people including a large ethnic Russian minority depends heavily on electronic services and that is why Estonia is also known as E-stonia. Estonia has e-government also known as paperless government and even the parliament is elected over the internet. Being highly dependent on electronic services, such a cyber attack against the country's IT systems can be catastrophic. According to the CERT Estonia, 98% of banking transactions are done electronically, 66% population uses the internet, 55% households have computer at home, and 91% computers are connected to the internet [6]. Furthermore, 2/3 of Estonians have broadband services, 80% fill taxes online.

The cyber attacks that were carried out were very coordinated and well planned which inflicted chaos across Estonia and Estonia was near to a halt of its critical business processes. Main targets of the attacks were:

- Estonian's Presidency and Parliament
- Government Ministries
- Political Parties
- Famous news organizations
- Banks
- Communication infrastructure

The attacks were so intensified that Estonia had to block foreign access to sites under siege. Some experts termed it as an onslaught of Estonia and security experts from NATO, European Union, Israel, and USA converged to Tallinn to help Estonia.

2.2. Facts and Figures

On April 27, 2007 first attack targeted the home page of the Foreign Minister Urmas Päts Free Market Liberation Reform Party. On June 6, 2007 SEB Eesti Ühispank (Bank) in Estonia was under heavy DDoS attack. Table 1 shows some of the facts of this cyber war [7].

Table 1. Targeted Websites

Attacks	Destination	Address or owner
35	195.80.105.107/32	pol.ee
7	195.80.106.72/32	www.riigikogu.ee
36	195.80.109.158/32	www.riik.ee, www.peaminister.ee, www.valitsus.ee
2	195.80.124.53/32	m53.envir.ee
2	213.184.49.171/32	www.sm.ee
6	213.184.49.194/32	www.agri.ee
4	213.184.50.6/32	
35	213.184.50.69/32	www.fin.ee (Ministry of Finance)
1	62.65.192.24/32	

The attacks were steady (recorded everyday during time period of the cyber conflict) in nature though weren't uniform (intensity varied on different days). The attacks lasted for three weeks and the number of attacks recorded is given in table 2.

Table 2. Number of Attacks

Attacks	Date
21	2007-05-03
17	2007-05-04
31	2007-05-08
58	2007-05-09
1	2007-05-11

Most of the attacks lasted from 1 minute to 1 hour while others were recorded for more than 10 hours that caused great damage to the target systems. Table 3 shows duration of attacks.

Table 3. Duration of Attacks

Attack	Time
17	less than 1 minute
78	1 min - 1 hour
16	1 hour - 5 hours
8	5 hours to 9 hours
7	10 hours or more

Bandwidth used for the attacks is given in table 4

Table 4. Bandwidth used for Attacks

Attacks	Bandwidth measured
42	Less than 10 Mbps
52	10 Mbps - 30 Mbps
22	30 Mbps - 70 Mbps
12	70 Mbps - 95 Mbps

The facts stated above are those that were detected and reported however original details may vary. Some data recorded on various days of the attacks is given below [9].

As the attacks started on Saturday, April 27, 2007, flows/sec increased dramatically, which mainly consist of UDP and TCP floods. Figure 1 shows the in and out traffic recorded on April 27, 2007.

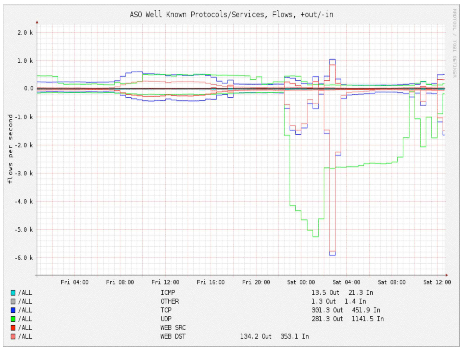

Figure 1. April 27, 2007

Figure 2 shows that the attack persisted and dramatic increase was observed on Monday April 30, 2007.

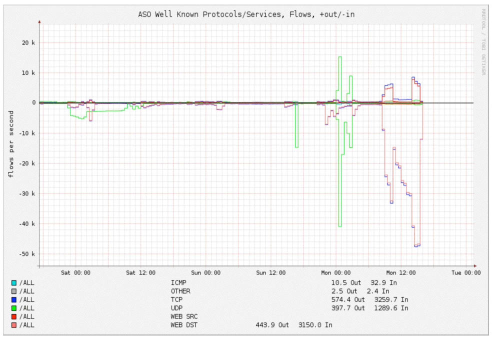

Figure 2. April 30, 2007

Figure 3 indicates that the amount of incoming traffic kept on increasing and heavy traffic was recorded on Thursday May 11, 2007.

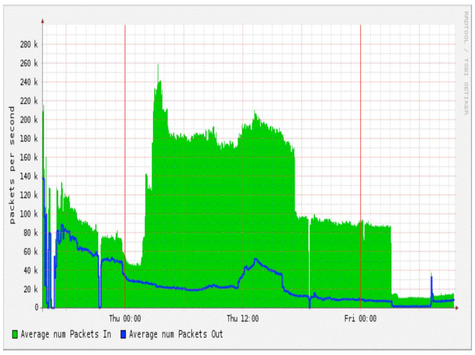

Figure 3. May 11, 2007

Figure 4 shows the statistics of incoming and outgoing traffic in packets/sec from April 28-30, 2007.

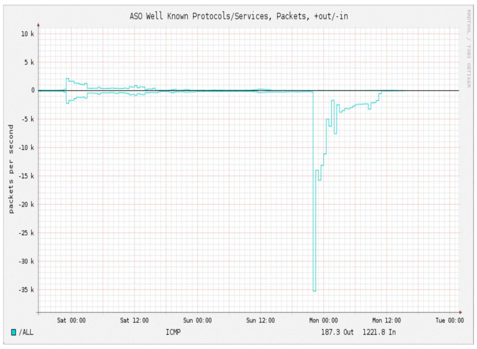

Figure 4. April 28-30, 2007

Figure 5 reveals the statistics of incoming and outgoing traffic in bits/sec from April 28-30, 2007.

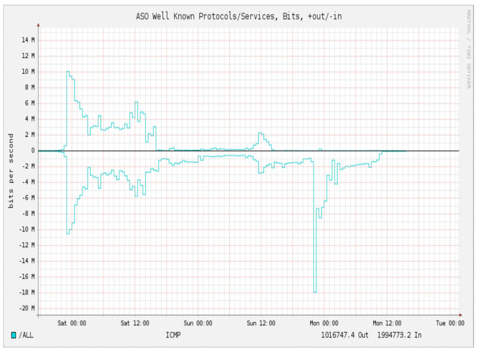

Figure 5. April 28-30, 2007

2.3. Tools and types of the attacks

The attacks carried out against Estonia were of DoS and DDoS type ranges from simple PING flood to more sophisticated botnets. According to the Asymmetric Threats Contingency Alliance (ATCA), Russia hired illegal botnets for short time to amplify the attack by involving million of computers in the assault on Estonia [8].

Data from Arbor Network Active Threat Level Analysis System (ATLAS), which claims to be able to monitor 80% of the internet traffic, reveals that 128 unique DoS attacks targeted IP addresses within Estonia over three weeks of conflict and most of which were ICMP PING flood that targets whole system instead of a particular port or service within the server [10]. Analysis of the ATLAS data also revealed that there were more than one botnets involved in the assault, making it difficult to track down the perpetrators. On the basis of the data collected from ATLAS, out of 128 unique DoS attacks, 115 were ICMP flood, 4 were TCP SYNC flood, and 9 were generic traffic flood [11].

There are lot of DoS tools available, some of which are for script kiddies and other for people with a little bit of experience. A good resource for hacking tools is [12]. Attacks on Estonia were quite heavy and most likely DDoS attacks were used in which attacker compromises large number of computers to launch heavy attacks. The attacker sends commands to a master computer that in turn forwards the instructions to daemon's installed on Zombies (victim computer) to launch heavy co-ordinated attacks against the target. Four well-known Distributed Denial of Service attacking tools are Trinoo, TFN, TFN2K, and Stacheldraht [13]. Trinoo sends flood of UDP packets without spoofing IP addresses that make it possible to trace back the source of attack. Tribe Flood Network (TFN) and its updated version TFN2K can generate different floods i.e. ICMP flood, UDP flood, SYN flood, and Smurf style attacks. In TFN, master communicates unencryptedly with daemon using ICMP ECHO REPLY packets to avoid firewall filtering, which was later updated with encrypted communication and one way spoofing in TFN2K. Stacheldraht works as a hybrid of Trinoo and TFN. Stacheldraht supports different types of floods just like TFN but on contrary Stacheldraht uses encrypted communication.

2.4. Techniques, Possible Defences and Tracing DoS attacks

As already mentioned that most of the attacks were ICMP and TCP SYN flood, in this section, first, ICMP and SYN flood attacks will be explained along with possible remedies. Furthermore, an overview of possible solution to trace back the perpetrator will also be included.

Internet Control Message Protocol (ICMP) is a fundamental part of TCP/IP protocol suite and is used for reporting network errors. ICMP messages are normally not authenticated and spoofing of packets is rather easy which makes it possible to launch a number of attacks against TCP i.e. connection reset, blind throughput reduction, and blind performance degradation attack. General defences against ICMP attack involves checking TCP sequence number in incoming ICMP packet to make sure that it belongs to an established connection. The ICMP message contains four-tuple namely source IP address, destination IP address, source and destination port numbers. Randomising port number to make it hard to guess also reduces the probability of spoof messages being accepted. Filtering ICMP messages based on payload that contains part of the TCP segment sent also reduces the probability of spoof messages being accepted. Furthermore, many implementations of the operating system discard ICMP messages silently. Firewall also filters ICMP messages to reduce risk of ICMP based attacks. In addition, there are attack specific defences implemented in firewalls and operating systems that help against ICMP attacks. For more thorough explanation of ICMP based attacks and possible mitigations, refer to [14].

TCP uses three-way handshake starting with SYNC message containing initial sequence number to initiate a connection with a remote computer. The remote computer responds with TCP SYNC acknowledge message and reserves some of the resources i.e. memory and bandwidth for new connection. The source computer doesn't respond to the target computer and keeps on sending TCP SYNC messages using spoof IP addresses at a rate faster than the target computer can handle. Eventually, resources of the target computer are exhausted with spoofed connection and victim cannot respond to legitimate TCP connections [15]. TCP SYNC flooding can be launched in number of ways and there are possible remedies. RFC4987 [16] outlines number of possible defences to counter TCP SYNC attacks. Spoofing of IP addresses is required in this type of attack and filtering based on IP address can effectively reduce the intensity of such an attack. Ferguson in RFC2267 [17] described in details that Network Ingress Filtering on ISP to stop IP address spoofing is an effective solution for DoS attacks. Increasing size of the backlog can also be helpful. Reducing SYNC Receiver Timer to discard half opened connections early is also a possible remedy to safeguard against DoS attacks. Using half opened connections for newly arrived connections (if further connection cannot be accommodated without using half opened connections) can effectively counter DoS attacks. Use of SYNC cookies that allocate resources only when connection is fully established is also a very effective solution but time consuming. Use of SYNC cache, hybrid approaches, firewalls and proxies can be used as possible shields against DoS attacks.

The Internet was not designed with taking into account tracing and tracking because it was to be used by trusted users to share information for research purposes. But with growth of the internet, more critical applications are being networked, pool of attackers increased and it thus becomes necessary to track down the perpetrators. Anonymous nature of the internet provides opportunities to hackers to carry out malicious activities without being detected or traced. Furthermore, it becomes very difficult to trace when attackers use compromised hosts to launch attacks against the target systems. Tracing the source of the attack is very important for two reasons. Firstly, to stop the attack in order to minimize damages. Secondly, to discourage such activities by punishing the perpetrator and learning about the techniques used for attacks in order to cover the loopholes to avoid future threats. Tracing perpetrator is a challenging and tedious task because IP header is not protected and attackers use spoof IP addresses to launch the attack. Techniques used and proposed for tracing and tracking are primitive in nature and further research is required for finding effective and efficient solutions. In addition, tracing also requires cooperation between different organizations to carry out traces inside their administrative domain if attacks originate from their domain and policies should be defined as to how to proceed with traces. Given below are some primitive techniques for tracing and tracking an attacker on the internet.

Hop-by-Hop IP trace back: This approach is suitable during the denial of service attacks involving a large flood of packets. Victim notifies ISP about the attack and ISP administrator then carries out debugging to find a router closest to victim through which the attack packets were routed towards the target. Then a router one step up is figured out which routes the attack packets to the router closest to the victim. This procedure continues until an input link from another ISP domain (through which attack packets are routed) are found and then ISP is notified of the problem and asked to carry out further tracing in their domain which requires cooperation.

Backscatter Trace back: This technique makes use of a large number of unassigned global IP addresses that are commonly used in DDoS attacks to flood target with spoofed IP packets. First, attack is reported to ISP and ISP configures its routers to block all the packets destined to victim. The routers which blocks the attack packets to the victim sends “ICMP” error messages to hosts having address as source address in rejected packets. ICMP messages with invalid destination address (unassigned globally) are routed to a specific machine named the ‘blackhole’ machine for further analysis. Source address of ICMP error messages are checked to identify router that acts as an entry point in ISP network for the attack packets. Filters, blocking packets destined for victim, are removed from all routers except the one that acts as an entry point for the attack. Finally, ISP asks the neighbouring ISP to continue trace back.

Robert stone suggested a technique which employs an overlay network over existing ISP network for hop-by-hop tracing and analysis [18]. The probabilistic approaches to traceback include ‘ICMP Traceback’ and ‘Packet Marking Scheme’ that are used in situations where there is a large number of packets flow. A very promising and effective approach for single packet trace is known as the ‘Hash-Based IP Traceback’ that stores a single compact value ‘Message Digest’ for each message calculated using the hash function [19].

3. News reports & Expert views

The attacks against Estonian IT infrastructure were given thorough coverage by the electronic and print media for this was the first major attack of its type. This section covers what was reported in newspapers and what are the expert opinions about the cyber conflict.

Newspapers reported it as just series of attacks that ended after three weeks of duration but experts were concerned about long term consequences and issues raised by this conflict. According to BBC [20] these were series of attacks carried out as a protest to deface government and other important websites. The famous British newspaper Telegraphy [21] reported “Estonia has been hit by a prolonged series of ‘cyber attacks’ that disrupted leading websites and caused alarm in Europe and the NATO alliance, it emerged last night”. In other words, Telegraphy termed it as the first cyber assault. Telegraphy also reported Merit Kopli, Editor of Postimees, one of the two main newspapers in Estonia, was quoted as: "The cyber-attacks are from Russia. There is no question. It's political“. The famous newspaper Dailymail [22] also termed these attacks as the first major attack of its type. British newspaper The Mirror [23] and Times [24] reported that tens of thousands of computers were involved in cyber assault. The USAToday [25] reported that fingers are being pointed at Kremlin for possible involvement. Fox News [26] also reported it as the first major cyber assault.

Newspapers reported it as an event that just occurred without addressing the long-term consequences and issues raised by information warfare. However, experts viewed it as the fifth dimension of war and alarmed IT companies to raise their security in order to avoid an undesirable mishap. Evron, one of the IT security expert involved to help Estonia, said, "While exact source of the attacks remain unknown, evidence suggests a highly organised assault". He added, "Public and political attitudes to cyber-crime must change, and law enforcement must be given greater resources to cope with its growing presence in the virtual community". Evron also suggested that "Different national law enforcement agencies and operations should collaborate and establish a common framework that will help trace recent developments involving internet security in a significantly faster fashion, as current measures have completely failed to cope". Evron was referring to the long-term security threat raised by information warfare and alerted that security awareness is very necessary to counter this problem.

The US Homeland Security Secretary Michael Chertoff "This attack went beyond simple mischief. It represented an actual threat to the national security and the ability of Estonian government to govern its country. We face in the 21st century a very difficult problem: a single individual, a small group of people and certainly a nation state can potentially exact the kind of damage or disruption that in past years only came when you dropped bombs or set off explosives". Though Chertoff exaggerated the damages of cyber assault but he was quite right that it is a threat that needs to be addressed. Colonel Charles Williamson, of intelligence and surveillance division of America's air force proposed, "America needs the ability to carpet-bomb in cyberspace to create the deterrent we lack. Botnet could be built out of obsolete computers that would otherwise be discarded but he conceded that there would be legal and political difficulties associated with its use". Many countries are believed to have cyber armies and others are developing cyber armies in order to use that during war as Colonel Charles was referring. The US IT experts say that Russia's cyber attacks against Estonia has given the whole world a wake up call. "If there are fights on the street, there are going to be fights on the Internet", said Hillar Aarelaid, Director of Estonia's Computer Emergency Response Team (CERT).

The general public are still unaware of the security precautions required though this event brought a short disruption of how day to day activities i.e. using ATM machines, paying online bills, online bookings, etc are affected by cyber attacks. However, experts are more concerned about the impact of cyber war in a broad perspective i.e. What if the electric power management system of a country or even a small region is taken over by an intruder? Critical systems i.e. transportation, stock market, medical care, telecommunication, banks, weather forecast, online government functions, etc are increasingly being networked and hacking into these systems can result in an immense impact on a country's economy, and even human lives will be at stake. In addition, experts believe that this conflict has alerted IT companies across the globe to enhance their security to avoid damages caused by cyber threats. Furthermore, experts suggest that governments should provide adequate security to safeguard its critical infrastructure against intruders and cyber terrorists. The documentaries [27] and [28] provide a detail of number of cyber incidents and experts views about the threat of cyber war.

4. Conclusion

Fear that IT systems could be used as an alternative way to spread terror and disruption was a concern since inception of IT systems but it became a reality after the April 2007 cyber assault. Though the damages caused by cyber attacks are yet to be seen but experts believe that such attacks are not that harmful as conventional and nuclear weapons. The cyber attacks are weapons of mass disruption rather than mass destruction. The cyber warriors are not restricted by geographical boundaries that mean you need a strong defence against an army that is always at your door. Government or border police can't control the cyber warriors and they are free to move everywhere and launch attacks anywhere without being detected in the anonymous nature of the internet. To add the worst, in cyber wars one does not know the capability of the enemy until they use them. Furthermore, experts believe that cyber wars may be used for political purposes.

In the end we must emphasize that cyber threat is inevitable and the cooperation of users, ISP's, CERT, Law enforcement agencies, common policies, and international cooperation is required to successfully deal with this potential threat to safeguard IT systems that play an immense role in our day to day life.

5. References

[1] Nathan Thornburgh, 'Inside the Chinese Hack Attack', Times, August 25, 2005. http://www.time.com/time/nation/article/0,8599,1098371,00.html

[2] "Estonia hit by 'Moscow cyber war', BBC, May 17, 2007. http://news.bbc.co.uk/2/hi/europe/6665145.stm

[3] Pete Swabey, 'Kyrgyzstan taken offline by Cyber attacks', January 29, 2009 http://www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=2156

[4] JOHN MARKOFF, 'Before the Gunfire, Cyber attacks', the New York Times, August 12, 2008 http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=1&em

[5] DK Matai, 'Cyber Warfare: Beyond Estonia-Russia, Rise of china 5th Dimension army for 21st C', May 30, 2007. http://www.intentblog.com/archives/2007/05/cyber_warfare_b.html

[6] “Facts about E-stonia”, CERT Estonia, May 10, 2008 http://www.ria.ee/27525

[7] Jose Nazario, “Estonia DDoS Attack”-A summary to date, Arbo Networks, May 17, 2008 http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/

[8] Iain Thomson, “Russia hired ‘botnets’ for Estonia cyber-war, May 31, 2007 http://www.infomaticsonline.co.uk/vnunet/news/2191082/claims-russia-hired-botnets

[9] Merike Kaeo, “Cyber Attacks on Estonia, Short Synopsis” http://doubleshotsecurity.com/pdf/NANOG-eesti.pdf

[10] Sean Michael Kerner, “Estonia under Russia Cyber Attack”, May 18, 2007 http://www.internetnews.com/security/article.php/3678606

[11] Beatrix Toth, “Estonia under Cyber Attack”, http://www.cert.hu/dmdocuments/Estonia_attack2.pdf

[12]http://www.viruslist.com/en/virusesdescribed?chapter=153318492

[13] “Distributed Denial of Service” Feb 2000, Watchguard Technologies, Inc. http://www.securitytechnet.com/resource/rsc-center/vendor-wp/watchguard/ddos.pdf

[14] F. Gont, “ICMP attacks against TCP”, October 27, 2008 http://tools.ietf.org/html/draft-ietf-tcpm-icmp-attacks-04

[15] “TCP SYNC Flooding and IP spoofing attacks”, November 29, 2000 http://www.cert.org/advisories/CA-1996-21.html

[16] W. Eddy, “TCP SYN Flooding attacks and common mitigations”, August 2007 http://www.ietf.org/rfc/rfc4987.txt?number=4987

[17] P. Ferguson, “Network Ingress Filtering”, January 1998 http://www.ietf.org/rfc/rfc2827.txt

[18] Robert Stone, “CenterTrack: An IP overlay Network for Tracking DoS Flood”. www.arbor**networks**.com/index.php?option=com_docman&task=doc_download&gid=96

[19] Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, and W. Timothy Strayer “Hash-based IP Traceback” www.ccert.edu.cn/upload/4/30.pdf

[20] “The cyber Raiders hitting Estonia”, Thursday 17, 2007 http://news.bbc.co.uk/2/hi/europe/6665195.stm

[21] “Cyber Attack, Hit Estonia”, May 18, 2007 http://www.telegraph.co.uk/news/worldnews/1551851/Cyber-attacks-hit-Estonia.html

[22] “Russia Launches Cyber war on Estonia”, May 17, 2007 http://www.dailymail.co.uk/sciencetech/article-455467/Russia-launches-cyberwar-Estonia.html

[23] “A war by Internet”, May 18, 2007 http://www.mirror.co.uk/news/top-stories/2007/05/18/a-war-by-internet-115875-19122853/

[24] “Estonia accuses Russia of ‘Waging cyber war’, May 17, 2007 http://www.timesonline.co.uk/tol/news/world/europe/article1802959.ece

[25] “Cyber attacks harass Kremlin critics”, May 30, 2007 http://www.usatoday.com/tech/news/computersecurity/cyber-attacks-kremlin-critics.htm’

[26] “Estonia's Web Sites Crippled by Russian Hackers”, May 18, 2007 http://www.foxnews.com/story/0,2933,273294,00.html

[27] http://video.google.com/videoplay?docid=-8100279136961358180

[28]http://www.youtube.com/watch?v=EuICZ0bsyvo