An Unsettling Trend

ATTACKS SHOW THE NEED FOR A PROACTIVE DEFENSE STRATEGY IN CYBERSPACE

Vytautas Butrimas, chief adviser, Lithuanian Ministry of National Defense

The 2010 United Nations Internet Governance Forum (IGF[1]) was held in Vilnius, Lithuania. Part of the IGF mandate is to "discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet." The IGF was meeting for the fifth time since 2005. The discussion was mostly set in the context of protecting privacy and freedom of access to the Internet.

Very little attention, however, was given to dealing with several disturbing cyber security events that occurred during the period of the IGF's five-year mandate. In 2007, for example, Estonia's Internet infrastructure was attacked to such an extent that the country was cut off from the Internet. In 2008, Georgia experienced a devastating cyber attack on its information and communications systems that resulted in the isolation of the Georgian government and people from the rest of the world. These attacks resulted in significant violations of privacy and freedom of Internet access, the very things that the IGF seemed so concerned about protecting.

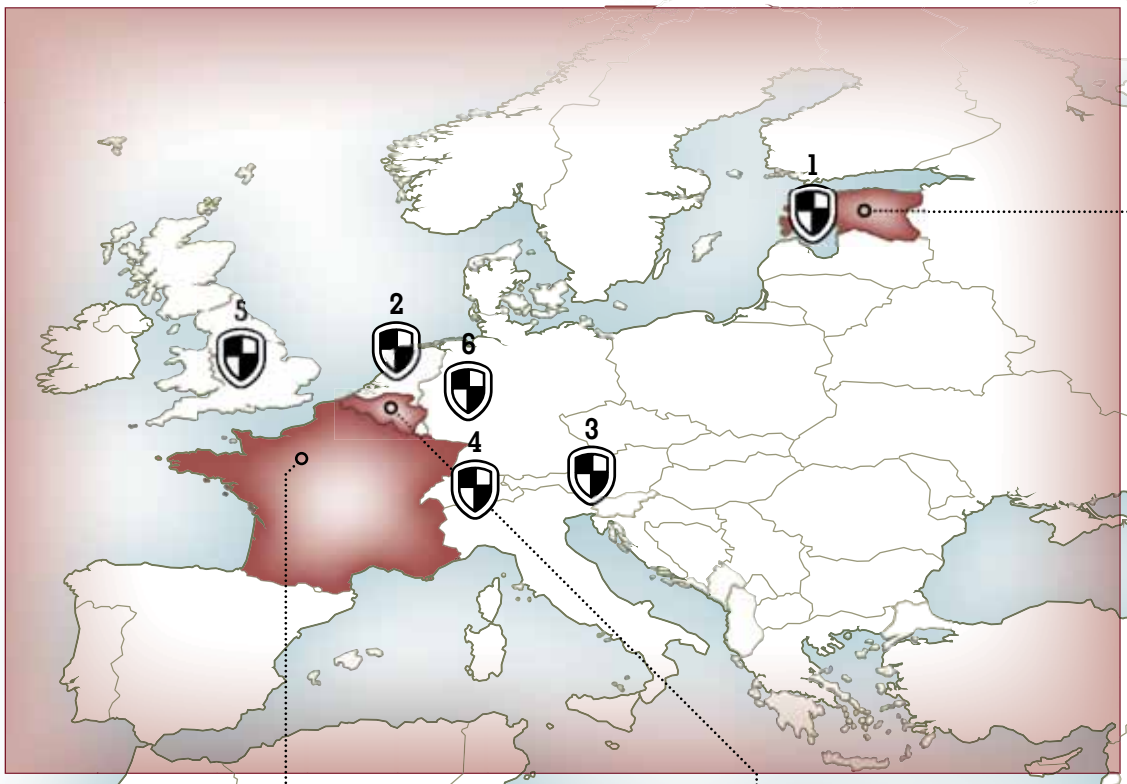
Something serious was going on in cyberspace. Unknown perpetrators were demonstrating sophisticated and effective cyber offensive capabilities against critical communications and information systems, or CCIS. Even more serious was that no one was held responsible for these attacks. This article will provide a brief appraisal of some important cyber events and trends in an effort to achieve a more balanced understanding of the cyber security issues facing the international community today.

MALWARE AND CYBER CRIME

The writing of malware (malicious computer software) and hacking[2] into computer systems is no longer an activity limited to amateurs or hobbyists looking for recognition. It has become a relatively safe and profitable criminal activity. One of the factors allowing for the development of this new growth industry of malware and botnets (robot computer network) is that the Internet or cyberspace is mostly a free and unregulated environment.

Think of it as a road or highway network. However, in this network, there are

Recent Cyber Attacks



Estonia
May 2007

Georgia
August 2008

Paris, France
Cyber attack prior to G-20 summit
December 2010

Brussels, Belgium
Major and widespread cyber attack before a large European Union summit to discuss the economy and the Middle East
March 2011

Iran
Stuxnet
Summer 2010

Sampling of Cyber Defense Agencies

1 **NATO**
Cooperative Cyber Defence Centre of Excellence
CCDCE

2 **The Netherlands**
National Infrastructure Against Cyber Crime
NICC

3 **Austria**
Austrian Program for Critical Infrastructure Protection
APCIP

4 **Switzerland**
Reporting and Analysis Centre for Information Assurance
MELANI

5 **United Kingdom**
Centre for the Protection of National Infrastructure
CPNI

6 **Germany**
National Cyber Defense Center
NCAZ

no rules of the road or police to issue "speeding tickets" or otherwise bring perpetrators to justice. Even if police existed, one would find it almost impossible to give them a description of the perpetrators. The perpetrator has long since left the crime scene, leaving no trace. This is the problem of attribution. It is very difficult to prove who did it. Perhaps the malware and botnet can be identified, but the criminal and his computer are safely hidden.

When Estonia was cyber attacked, its specialists had a gut feeling who was behind it, but finding proof was one of the first problems. The first list of attacking computers were identified in unexpected countries such as Egypt, Vietnam and Peru.[3] Most likely, these computers were part of a botnet controlled by a "herder" who had previously installed his software on poorly secured personal computers throughout the world.

Money can be made by using malware to commit fraud, break into banking systems and take control of people's credit card and banking accounts. Cyber crime is on the rise. A report by the U.S. National White Collar Crime Center noted more than 330,000 cyber crimes in 2009, an increase of 667 percent since 2001.[4]

The malware that can attack and hack into these financial systems has a value much like any commodity. A "herder," or commander, of a botnet makes use of malware to infect and control other computers. Botnets are sold and rented just like any commodity, with prices based on supply and demand.[5] A new industry has therefore emerged as one of the fastest growing sectors in the criminal world. Professional skills are required to hack into a computer and run a botnet. These skills are very much in demand not only in the cyber crime economy but also in government and private sectors.[6]

SOCIAL NETWORKING THREATS

The next trend on the rise is social networking. The Internet has provided new ways for people to stay in touch and share information. Pictures, videos and files can be shared freely, either publicly or with an authorized group. Social networking also lends itself to social activism. On Facebook, for example, there is a section labeled "causes" where interested parties can meet and organize. If you are unable to find a cause, you can search for it or create one. These causes provide possibilities for healthy democratic activism, but what if that activism is destructive?

In one published case,[7] a website called for "volunteers" to fight a cause. Those who wanted to "join the fight" only had to download the provided software and the software would do the rest. In effect, those people allowed their computers to join a botnet.

Social networking offers like-minded people a chance to act together for democracy, but it has a dark side. For example, an individual or group could use these services to raise volunteer armies of cyber warriors. The process is as simple as following written instructions or downloading someone's malware. In 2007, we started to see this in action.

CYBER ATTACKS: ESTONIA AND GEORGIA

The year 2007 marked a watershed in cyberspace. The Estonian example demonstrates that a cyber attack on a nation's infrastructure, initially fueled by a grassroots patriotic base, can later attract professional cyber criminals. It's a potent combination.

On the surface, the cyber attack seemed to be a spontaneous and patriotic Russian reaction to Estonia relocating a statue of a Russian Soldier. However, the attacks showed a degree of organization that was adequate to cripple Estonia's internal networks

TIMELINE

OF COMPUTER AND INTERNET ADVANCES AND SETBACKS


APPLE

1976:
Apple Computer founded, marking the start of the age of personal computers.


WIKIPEDIA

1981:
Microsoft Corp. offers its first computer operating system to the public.

1984:
The European Organization for Nuclear Research (CERN) begins installing a version of the Internet to link its internal computers.

and Internet links temporarily. Targeting and attack information was provided on websites to those who wanted to use their computers to enter the fray. Botnet managers that had used malware to infect unsuspecting computers directed their "zombie" computer armies to "open fire" against listed Estonian banking, government and press sites.

In August 2008, the use of linked computers to temporarily disrupt a nation's CCIS infrastructure took on a new and potentially deadlier form — the execution of a cyber attack during a traditional military operation. It combined several elements used in the Estonian attack a year earlier: grassroots patriotism channeled with the help of social networks, professional botnet herders and elements of organized crime. The result was the execution of a well-planned, well-timed and debilitating cyber attack against Georgian government and civilian CCIS. This attack succeeded in cutting off access to information about what was happening in the country. Daily business was disrupted, and people were fearful and uncertain what would happen next. In short, Georgia's ability to organize and coordinate its national defense was severely compromised.

A study of the cyber attack in Georgia also suggested the appearance of a darker trend — the possibility for physical destruction of critical CCIS components.[8] According to the study, a much more deadly attack could have been executed; however, the perpetrators chose restraint.[9] Unfortunately, the organizers of the attack learned an important lesson: It's still an attractive weapon and nobody has a clue how to deal with it.

THE ASSOCIATED PRESS

The Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, was created by NATO to enhance capability, cooperation and information-sharing among member nations and partners.

STUXNET: FIRST INTERCONTINENTAL CYBER ATTACK?

The appearance of the Stuxnet malware in 2009, and its appearance in the news in the summer of 2010, revealed a new cyber stew combining the ingredients of the cyber professional's skills. Publicly available analysis of Stuxnet indicated that this was a well-researched and sophisticated worm. The worm demonstrated it could not only temporarily neutralize a target, but destroy it physically.

One study suggests[10] that the substantial resources (cyber professionals and intelligence assets) required to deploy this worm could be supplied only by a government. One of the intended Stuxnet targets could have been Iranian nuclear facilities whose supervisory control and data acquisition systems (SCADA[11]), used to manage sensitive operations, were manufactured by Siemens.

THINKSTOCK

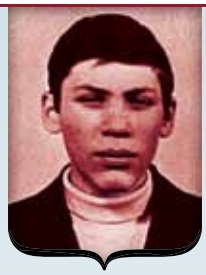
1986:
First case of successful attribution. Astronomer Clifford Stoll uncovers KGB hacking of U.S. SDI data.

ROANOKE COLLEGE

1989:
The firm McAfee Associates markets its first anti-virus software. Internet attracts its first 1,000,000 users.

THINKSTOCK

1991:
World Wide Web (www) formally established.



1994:
Russian hacker Vladimir Levin robs major corporations by breaking electronically into Citibank accounts.

It was difficult to determine if Stuxnet succeeded in performing the destructive task it was designed for. It appeared in other countries and there were no reports about damage to nuclear facilities.

One study concluded that Stuxnet was designed as a psychological weapon and as such was probably successful.[12] Imagine being able to deliver the following message to your adversary: "We don't like what you are doing with this facility, we can control it without your knowledge, and by the way, maybe you should be careful about pushing buttons." As with previous cyber events, the organizers of Stuxnet remain unknown. There may be no "smoking gun," but there is "blood in the water."[13] If Stuxnet and its variants are a new form of cyber attack, this represents a new trend and deeper problem.

BURMA'S ELECTORAL ATTACK

Burma, in the first week of November 2010, was preparing for its first national elections in 20 years. The elections received plenty of press coverage, but one event almost went unnoticed. One week before the elections, Burma CCIS infrastructure suffered a massive distributed denial-of-service[14] attack, effectively cutting Burma off from the Internet. One can only speculate on what effect this attack had on the Burmese elections. In cyber security terms, however, this attack demonstrated a disturbing escalation in cyber attack capabilities. The attack against Burma was several times more massive than the attacks against Estonia and Georgia.[15] This increase in "cyber power" constitutes a troubling trend.

CONCLUSIONS

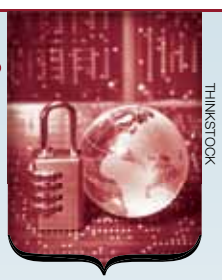
The state's dependence on CCIS and its vulnerability to disruption or destruction via malware sent from unknown locations by unknown perpetrators has created a new and attractive form of attack. Such an attack is attractive especially for governments unable to achieve a foreign policy objective using internationally acceptable means.

This Internet option provides so many levels of application that it is too tempting for a state not to use. It can be employed clandestinely through third parties with the assurance of nearly 100 percent deniability, regardless of whether the attack becomes publicly known. Harm can be limited to just short-term disruption or expanded to damage CCIS physically. The "commanders" of these arsenals are hidden but are reachable by those interested in employing their services. One can harp on the fact that there is no "smoking gun" proving government involvement but circumstantial evidence can build a good case that governments are involved to some degree.

To the extent that botnets and malware can disrupt the state's critical CCIS infrastructure, the cyber threat is a national security issue. This is recognized by nations dependent on the Internet and those seeking to take advantage of that vulnerability. In recognition of the threat, governments are beginning to cooperate in fighting cyber crime. However, many are also competing in a cyber arms race.[16]

Industry can inadvertently make it easier to mount cyber attacks. For example, Microsoft Corp. announced it had signed a Government Security Cooperation Agreement with Russia that, among other things, provided access to the Windows operating system source code.[17] The company signed the same agreement with China in 2007[18] and, this past summer, provided the Russian government with access to the code of the latest Windows operating system. One can perhaps understand the marketing and sales motives behind Microsoft's actions, but it's not hard to understand that if the code falls into the wrong hands it could be used to find weaknesses and new attack vectors for exploitation.

How can we address this new threat to national security and avoid a possible cyber arms race? For starters, government and industry need to understand their dual roles in being part of the solution and part of the problem. Restraint within the framework of a "cyber arms control treaty" could be considered. Treaties, however, need to be verifiable and enforceable to be effective. Principal stakeholders among



1995:
The Strano Network becomes one of the first "hacktivist" groups when it attacks French government computers.

1996:
Finland's Nokia launches the first cell phone with Internet connectivity.

1998:
Google establishes its first search engine.

2000:
10 million Internet domain names registered up to this point. The Love Bug "worm" from the Philippines corrupts computers worldwide.

the public and private sectors and international community need to be identified, and appropriate coordination instruments need to be applied. The objective would be the creation of an intelligence-gathering and communications network that would allow for the exchange of information leading to the identification of cyber criminals and attack organizers. This means coming up with a reliable solution to the problem of attribution. If it is possible to pin down who is attacking then perhaps those gray commanders would be forced to weigh the costs and benefits of an attack. Once the organizers of the attacks have been identified, an international instrument needs to be on hand to ensure enforcement and punishment, if necessary.

Call it an Internet police[19] force, if you will. Nations must hold service providers and individuals accountable for their actions. If they do not agree to act on information, sanctions should be applied. We must raise the price for those wishing to organize cyber attacks.

International action will take time, but a step can be taken now at the local level: creating a cyber specialist contact network composed of all sector players (government, the private sector, banking, energy, transportation, commercial interests and telecommunication). Government must lead, since it should naturally be concerned with developing a national cyber security strategy.

This league of experts representing all cyber security stakeholders could be the first national line of cyber defense. The contacts forged during meetings and consultations will increase trust among stakeholders to share information and expertise that can be tapped during a cyber emergency. Memorandums of understanding for cooperation among stakeholders would allow for a more coherent and coordinated response to incidents.

One should not wait for a crisis and respond to it *ad hoc*. In May 2007, at a joint NATO-Microsoft workshop on cyber security held in Redmond, Washington, the Estonian representative came to the podium and announced "my country is under cyber attack." After a night of phone calls to capitals, offers of help eventually came but everything was done impromptu. Since then, some progress has been made beyond the *ad hoc* approach to cyber crisis management.

Cyber security and the Internet are at a crossroads. The way we deal with cyber security today will determine not only the extent to which privacy and freedom of access will be preserved but the security of our CCIS as well. It is not enough, however, to concentrate on cyber crime or restricting terrorists use of the Internet for information or recruitment purposes. To paraphrase Sun Tzu, the enemy (as well as ourselves) must be fully understood if we are to prevail. □

1. http://www.intgovforum.org/cms/aboutigf
2. People committed to circumvention of computer security. This primarily concerns unauthorized remote computer break-ins via a communication networks such as the Internet (Black hats), but also includes those who debug or fix security problems (White hats), and the morally ambiguous Grey hats. http://en.wikipedia.org/wiki/Hacker_(computing)
3. Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," Wired magazine, Issue 150 2007-08-21. http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all#ixzz0mIn5gsPQ
4. 2009 Internet Crime Report, NWCCC and US DoJ, p.15, http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf
5. http://www.businesscomputingworld.co.uk/botnets-for-rent-explained/ and http://www.net-security.org/secworld.php?id=4002
6. "Marc Maiffret: The quick rise of a teen hacker," http://news.cnet.com/8301-27080_3-20002317-245.html?tag=mncol
7. Gunter Ollmann, Damballa "The Opt-In Botnet Generation," p. 13., 2010. http://www.damballa.com/downloads/r_pubs/WP_Opt-In_Botnet.pdf
8. "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008." p. 5, 2009 U.S. Cyber consequences Unit, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf
9. Ibid. p. 5.
10. Preliminary Stuxnet report ver. 1, p. 16., The cybersecurity forum initiative, 2010 http://www.csfi.us/
11. SCADA – supervisory control and data acquisition, http://en.wikipedia.org/wiki/SCADA
12. Preliminary Stuxnet report ver. 1, p. 16., The cybersecurity forum initiative, 2010 http://www.csfi.us/
13. http://www.zdnet.com/blog/security/metasploit-and-scada-exploits-dawn-of-a-new-era/7672?tag=nl.e589
14. Distributed Denial of Service (DDOS)
15. Craig Labovitz "Attack Severs Burma Internet," November 3rd, 2010, Arbor Networks. http://asert.arbornetworks.com/2010/11/attac-severs-myanmar-internet/
16. Jim Wolfwed, "China aims to top U.S. in cyberspace," U.S. general, International Business Times, 13 June 2007 http://www.ibtimes.com/articles/20070613/china-internet.htm
17. Tom Espiner, ZDNet UK, 8 July, 2010 "Microsoft opens source code to Russian secret service" http://www.zdnet.co.uk/news/security/2010/07/08/microsoft-opens-source-code-to-russian-secret-service-40089481/
18. AsiaInfo Services 08-07-2007, "Microsoft signs new open source code agreement with China," www.highbeam.com/doc/1P1-142370666.html
19. "Where are the Internet police?" Data Center Times, 2009-03-03, http://www.datacentertimes.com/view_article.php?a_id=64&PHPSESSID=f134dc43445920bfdf69622e2c0b3cee


AGENCE FRANCE-PRESSE

2001:
Scottish hacker Gary McKinnon breaks into dozens of defense computers in what is called "the biggest military computer hack of all time."


THINKSTOCK

2007:
Web users exceed 1 billion mark worldwide.

2009:
Chinese computer spying operation dubbed Ghostnet discovered infiltrating machines in more than 100 countries.

2011:
"Anonymous" group hacks Sony and Bank of America servers, exposing confidential information to the public.