



Estonia and Cyberwar – Lessons Learned and Preparing for the Future

By White Wolf Security

In the early part of April of this year, the country of Estonia was attacked in cyberspace. While there has been much to do about the event in the press there are some very important issues that are being missed. First and foremost, nothing about the attack (including its duration) is new. Second, the attack is noteworthy because it was not coordinated by the Russians. This puts strategic cyberwarfare in the hands of non-state actors. Third, there are things we can do to prepare for eventual future attacks.

Part I - Nothing in the attack was new

To those in the business of information security and assurance, nothing about the attack, how it was conducted and the technologies used, is new. The attack is standard bot-net distributed denial of service attacks (DDoS). DDoS are a tried and true form of internet extortion and attack. We have seen large scale attacks against the US military infrastructure (“Network Attack Disables Naval War College, <http://www.fcw.com/article96957-11-30-06-Web>) and private companies. In fact, attacks of this type drove an Israeli company out of business (“Blue Security Folds Under Spammer’s Wrath, <http://www.securityfocus.com/news/11392>).

The power of a bot-net lies in its size, simplicity and synchronicity. In the physical realm, the hardest attack is one that coordinates operations in multiple geographic regions with simultaneity in attack time and target. A bot-net solves these issues very well. A single command in a handful of chatrooms send the exact same order to every member of the bot net. In the case of the DDoS attack, the order is simple; ‘at a specific time, continually send large amounts of traffic to the following target or targets’.

Using a very quick von Clausewitz analysis, here’s how the attack measures up:

1. Objective – Deny legitimate traffic to specific servers in Estonia
2. Offensive – In the US Army’s definition of ‘seize, retain and exploit the initiative’. Under current international law and policy, victims of a cyber attack are not allowed to counterstrike...it is very easy to keep the initiative when the target is only allowed to be defensive.
3. Mass – This is the primary weapon of a DDoS attack. Under the best of days, there are few infrastructures that can withstand the mass of a one million bot attack.
4. Economy of Force – Botnets are the quintessential economy of force; they can be run by one or two people. One bot-herder orchestrates and manages the bot while other members of the attack team are free to attack in other, less obvious or mass-centric ways. Essentially any keyboard is the general for million bot army.
5. Maneuver – The US Army definition works again here. From FM-100-5 (1994), maneuver is defined as: “Place the enemy in a position of disadvantage through the flexible application of combat power”. The



defensive only action of the victim, combined with the ability to vary the type and origin of every attack give the attacker the upper hand in its freedom to move. The Estonia servers are fixed by their IP address, even if they move, they become fixed in cyberspace again when they acquire new IP addresses. The defender (in cyberspace) is *always* in a static, fixed defensive posture. The attacker is always fluid, flexible and dynamic.

6. Unity of Command – Again, the botnet is elegant for this. Since a single person directs the botnet, there is a single commander for the attack.
7. Surprise – In cyberspace and its defense only rules, the attacker is always granted the element of surprise. The attacker chooses the time, the target and the method of attack.
8. Security – This focuses on the attacker’s ability to keep their plans unknown until the attack is underway. There is a vast number of ways for coordinated attackers to keep their plans to themselves. Also, the attack code used in botnet attacks rarely lists the intended target(s). A bot is merely an attack platform, it will engage target(s) when and how it is directed to by the bot-herder.
9. Simplicity – Keep the objectives clear. DDoS attacks are, by definition, simple. Fill an internet connection with more traffic than it, the routers or the servers can manage.

Part II – Strategic Weapons in Non-State Hands

The fact that the attack against Estonia was not state sponsored is even more chilling than if it had been an open act of state aggression. For the past 10 plus years, the world has seen most nations develop military based information operations units. The nations in this list are of varying degree of industry and wealth. We expect that most nations either are developing or have developed the ability to conduct offensive operations in cyberspace. Similarly, we know and expect the private sector to engage in its own brand of warfare. Organized crime regularly targets companies and private networks for theft, extortion, etc. What we see in the Estonia attack is the first incident of a private sector actor(s) attacking a state with strategic impact. Furthermore, since this is most likely the act of individuals instead of a government, the attackers are shielded through a maze of legal issues involving jurisdiction, extradition, trial and punishment.

The second chilling part of this fact is that our enemies learn from each other. Botnet attacks are cheap when compared to conventional strategic weapons. Any Al-Qaeda cell has the financial means to purchase a time limited DDoS attack against any target on the internet. Most believe that this is contrary to the traditional need to create blood, bodies and terror. However, when you combine a targeted DDoS attack against critical infrastructure and couple that with the core competency of terrorism, bombings; you have a very real and very dynamic result.

A concerted DDoS attack is an excellent force multiplier for a traditional physical attack. With technology convergence, DDoS attacks are not just for websites. Cell phones, pagers and other mobile communication devices are susceptible to denial of service attacks.



Part III – How to Prepare for the Future

There are two primary principles for the future:

1. The best defense is a good offense

At this time, the modern world (with few exceptions) believes that counter attacking, cyber self defense or active defense is illegal. I am not aware of any national or international agreements, laws or treaties that require a nation to stand by and let its citizenry and infrastructure to be freely attacked. Use of cyberforce in the defense of a nation and its populace is no different than the use of physical force. (For a complete discussion on this please see *Offensive Operations in Cyberspace* by White Wolf Security - http://www.whitewolfsecurity.com/offensive_ops.asp). A sovereign nation is allowed to take reasonable steps in the protection of itself. It is time we start doing so.

2. Train as you fight, fight as you train.

This is not the first multi day attack that we've seen, nor will it be the last. The owner/operators of IT infrastructure need to start thinking about ways to train that will realistically prepare them for a protracted and directed attack. The best training model for this is the military exercise. The military is very adept as multi-day exercises. These exercises not only test the equipment our forces use to fight, but also build the unit cohesion and leadership skills that no amount of technology can replace. The exercises have aggressors and defenders, missions and op orders. Best of all is the after action review. A process that formalizes the debriefing process and maximizes lessons learned. White Wolf Security offers its MANTA (Multi-day Active Network Tactical Assault) exercise. MANTA is an around the clock exercise that focuses on several core combat principles

- Leadership
- Communication
- Crisis management
- Unit cohesion
- Decision making under stress
- Technical proficiency under fire

We must treat our IT professionals as combat personnel and train them accordingly. Not just in skill, but in spirit too.