The Looming Threat of Cyberwar: Why India needs to be Prepared

Shivnath Babu
Assistant Professor
Department of Computer Science
Duke University
Durham, North Carolina, USA
shivnath@cs.duke.edu

The havoc caused by the recent terrorist attacks in Mumbai show how vulnerable India is to such attacks. Our citizens and politicians are now lamenting the absence of measures that could have prevented this attack or blunted its impact. This article attempts to highlight why India should be prepared to handle another omnipresent threat, *cyberwar*. While cyberwar will not cause physical injury on the scale of the Mumbai attacks, this new type of warfare can be more destructive from a financial and economic perspective.

Cyberwar is the use of computers and the Internet in conducting warfare. Before taking a look at the methods of cyberwar, let us look at the more general problem of *cybercrime*. Cybercrime denotes criminal activity where a computer or a network of computers is the target, source, or venue of a crime. Such crime includes unauthorized access to a computer or illegal interception and tampering of data sent over the network from one computer to another. Perpetrators of cybercrime are usually called *hackers*. There has been a spate of incidents recently where hackers stole credit card information of unsuspecting people. The stolen information was then used to make unauthorized purchases of goods on the Internet.

Cyberwar is a vicious form of cybercrime that has reared it ugly head in recent years. The target victim in a cyberwar is not a single individual, but a large company or an entire nation. The *Estonian cyberwar* is a prominent example that occurred in 2007.

The Estonian Cyberwar

The Republic of Estonia is a democratic parliamentary republic in the Baltic region of Northern Europe. Estonia is bordered to the north by Finland across the Gulf of Finland, to the west by Sweden across the Baltic Sea, to the south by Latvia, and to the east by the Russian Federation. The capital and largest city is Tallinn. Estonia is a member of the European Union and NATO.

Estonia is one of the early and thorough adopters of modern Web technology. More than 40% of Estonians use the Internet to read newspapers daily. More than 90% of bank transactions are done over the Internet. Credit card transactions made through a cell phone can be used for shopping. The country is saturated with free Wi-Fi (wireless Internet access), and is home to the rising Internet-based phone company, Skype. Estonia has successfully pursued the development of e-state and e-government. Voting through the Internet is used in local as well as parliamentary elections. Estonia now has one of the strongest economies of the new member states of the European Union.

On April 27, 2007, the Estonian government decided to remove a 6-foot-tall bronze statue that was located in the heart of Tallinn. This statue was a monument built by the Russians in 1947 to commemorate their war dead after driving the Nazis out of the region at the end of World War II. Having rid the country of Nazi occupation, the Russian secret police moved in. In the years that followed, a number of Estonians were deported to Siberia. Therefore, the statue was a symbol of an oppressive regime to many Estonian citizens. After many years of independence, the Estonian government had finally defied the Russian government---which had warned of negative consequences---and uprooted the statue. The statue was later installed in a military cemetery in the suburbs of Tallinn.

The Estonian government’s decision led to violent protests in Tallinn. Protestors smashed shop windows, destroyed cars, and threw rocks at riot police. Most of the protestors were ethnic Russians, who make up a quarter of the nation’s population. But the protests died down quickly.

As the protests within Estonia subsided, a different kind of aggression began to sweep the nation. The Web site of Estonia's leading newspaper became inaccessible all of a sudden. Within a matter of seconds, the Web sites of all prominent newspapers went down. The problem did not stop with the newspapers. The leading bank was no longer accessible over the Internet. All government communications went down soon after. However, everything was quiet on the outside. The border security personnel saw no incursions over Estonia’s borders with its neighboring countries. The Estonian airspace and territorial waters had not been violated. However, it was clear that some invisible enemy had invaded Estonia.

It took some time for the Estonian military and police to realize what had happened. Estonia was under attack by a *botnet* consisting of a large number of computers hijacked by hackers. These hijacked computers were not just in one single country, but spread throughout the world in places as far flung as Egypt, Peru, and Vietnam. The primary modus operandi of these computers was the ping attack---a simple request for a response from a computer on the Internet, but repeated hundreds of times per second. When deployed by masses of attackers, the pings can overwhelm the target computer and make it accessible by legitimate users. The botnet had slipped into Estonia through its least protected border---the Internet.

“The attacks were aimed at the essential electronic infrastructure of the Republic of Estonia,” says Jaak Aaviksoo, Estonia's minister of defense. “All major commercial banks, telcos, media outlets, and name servers---the phone books of the Internet---felt the impact, and this affected the majority of the Estonian population. This was the first time that a botnet threatened the security of an entire nation,” Aaviksoo says. The attack crippled life in Estonia. People could not shop, read newspapers, or access their bank accounts. These things were not just minor inconveniences, but a major hassle since the Internet had become part and parcel of daily life.

Who was behind the Attack?

There is a lot of evidence to suggest a Russian hand behind the Estonian cyberwar. Estonia has pursued a foreign policy of close cooperation with its Western European neighbors. Estonia's international realignment toward the West has been accompanied by a general deterioration in relations with Russia. These relations nosedived in the aftermath of the relocation of the bronze soldier memorial. Russian-language chat rooms on the Internet show how incensed many Russians were about the relocation of the memorial. There were hundreds of messages calling for a coordinated attack through the Internet on Estonia. The Russian government has, however, denied any involvement in the attack.

It is not the first time that the Russian government had been accused of being involved in a large botnet attack. Just a few weeks earlier, a similar assault had been launched against an alliance of Russian opposition parties led by chess grandmaster Garry Kasparov. Denis Bilunov, the executive director of Kasparov's party, the United Civil Front, alleges that there is a specific department within the FSB---the successor to the notorious KGB---that specializes in coordinating Internet campaigns against those whom they consider a threat. “They have attacked Chechen rebel sites, us, and now it appears they have attacked Estonia,” Bilunov says.

The Estonian cyberwar is not the first botnet strike ever, nor is it the largest. However, this incident is the first time an entire nation has been targeted on almost every digital front all at once. The United States has come under repeated attack from computer networks in China and Russia. The e-mail of the Office of the United States Secretary of Defense has been compromised by hackers. The United States White House had to deal with unidentifiable intrusions in its networks recently. China has been accused of cyber-attacks on India, Germany, and the United States. The computer network of the Indian Ministry of External Affairs was broken into in April 2008, allegedly by Chinese hackers. In fact, over the last two years, Chinese hackers are alleged to have mounted almost daily attacks on Indian computer networks, both governmental networks and those in the private sector. China denies knowledge of these attacks. Recently, Georgia fell under cyber attacks during the 2008 South Ossetia War with Russia.

Estonia could barely stay on top of the botnet attack by shutting down all its network connections with the rest of the world. Ironically, though this attack was a 21st-century attack, Estonia had to fall back on the same defense that they had used against Russian invasions four centuries earlier: close the gates, pull up the ramparts, and settle in for an indefinite siege. The problem with this approach was that Estonia could not convey to the outside world what was going on in the country; Estonians were shut out from the rest of the world. In mid-May 2007, the major botnet attacks stopped as suddenly as they had started; but considerable damage had been done to the Estonian economy and pride.

The Lessons for India

What are the lessons for India from the Estonian cyberwar? Over the part few years, India has embarked on an aggressive program of modernization based on computerization and Internet expansion. The main government organizations are now interconnected, railway and airline reservations can be done over the Internet, and major banking facilities are available 24x7.

The Indian government is using the Internet to facilitate administration. Such measures of e-governance can greatly enhance existing efficiencies, drive down communication costs, and increase transparency in the functioning of various departments. E-governance also gives citizens easy access to tangible benefits, be it through simple applications such as online form filling and bill payments, or complex applications like distance education and tele-medicine. Law enforcers now depend on the Internet to communicate across state boundaries as well as to share information on crimes and criminals.

The benefits of the Internet age are going beyond Indian cities thanks to ambitious programs like e-Choupal. e-Choupal is an initiative of ITC Limited (a large business conglomerate in India) to link directly with rural farmers for procurement of agricultural and aquacultural produce like soybeans, wheat, coffee, and prawns. ITC Limited has now established computers and Internet kiosks in rural areas across several agricultural regions of the country, so that farmers can negotiate the sale of their produce directly with ITC Limited. The computers and Internet access at these kiosks enable farmers to obtain timely information on prices, good farming practices, and place orders for agricultural inputs like seeds and fertilizers.

While India's program of computerization and interconnectivity has made our lives easier, it leaves us more vulnerable than ever to an all-out cyberwar. India has more than its share of enemies. The Estonian cyberwar shows that an enemy organization or country could launch a botnet attack to swamp the Web sites of Indian organizations including our parliament, ministries, banks, newspapers, transportation facilities, and broadcasters. Given how dependent India is on its Information Technology (IT) industry, a cyberwar can paralyze our economy. We cannot afford to shut our doors on the outside world; a measure like that could result in unprecedented losses for Indian companies.

To deal with the threat of cyberwar, we need to proactively create an infrastructure to prevent them as well as to cure them. Nowhere before has the statement “an ounce of prevention is worth a pound of cure" been more true than it is in the case of cyberwar. However, given the range of sophistication that hackers display these days, it would be foolish to focus only on preventing cyberwar; cure is also important.

Recall that Estonia's approach to deal with its cyberwar was to shut down its Internet connections with the rest of the world. While this measure protects against hijacked computers from the rest of the world, it is still vulnerable to threats from computers inside our own network. The more serious problem is that the Internet connection to the rest of the world is required for many legitimate uses.

Better ways to deal with an ongoing cyberwar come from an in-depth understanding of the common attack modes and tools. These include the ping attack discussed earlier---which comes from the larger family of distributed-denial-of-service (DDoS) attacks---and the techniques used to hijack computers and to organize a set of hijacked computers into a botnet. A key logger is a common piece of software used to hijack computers. Key loggers scan computers the moment a key is hit on the keyboard. This information is conveyed immediately to an external controller---so the controller not only knows the password on the computer, but is also notified when the password is changed. Key loggers are an example of malware (malicious software) that gets installed automatically on computers when users are not careful. We need to develop and use good protection tools that can quickly detect and eliminate malware used in cyberwars.

The Indian Defense Ministry has long developed plans of action to combat air raids, missile attacks, naval bombardment, and tank advances by enemies of the nation. In a similar manner, strategic planning must be done to combat cyberwar. We should keep in mind that cyberwars spread much faster than the speed at which armies, navy, or the air force can move. Hence, a rapid response team is a must.

Our government should realize that it does not control the whole Internet, so it cannot effectively combat a cyberwar on its own. In fact, no country can protect itself from cyberwars on its own. There needs to be broader international consensus and cooperation. Given India's vulnerability, it is in our interest to initiate steps to create an international platform for combating the threat of cyberwar.

At the same time, Indian citizens should be made to understand that the security of our computer infrastructure in the modern Internet age is not exclusively a governmental responsibility. It is a shared responsibility. The private sector as well as people who run critical infrastructure and manage our key resources should share the burden of this responsibility. It is also a responsibility held by each one of us who use personal computers and browse the Internet at home and office.