Battling Botnets and Online Mobs

Estonia's Defense Efforts during the Internet War

Gadi Evron

What would happen if tomorrow the Internet ceased to function? To most critics, and particularly state officials and policy makers, the possibility that the Internet could one day suddenly disappear is no more than a mere speculation, a highly improbable concept. On May 2007, the events that took place in Tallinn, the capital of Estonia, proved everyone wrong. On that day, Estonia fell victim to the first-ever, real Internet war. This article delves into the political context that shaped the incident and analyzes some of the key lessons and policy implications that emerged as a consequence.

Gadi Evron is security architect for Afilias Global Registry Services, a cyber-crime expert, and a recongnized leader in Internet security.

The Roots of Anger. Estonia's difficult past—World War II, the Soviet occupation, Cold War, and post-communist transformation—set the stage for the conflict that ultimately erupted in Tallinn between its Estonian and Russian citizens. Estonia's relationship with its large Russian minority dates back to World War II, when the Soviet Union annexed the Baltic States in the 1939 Molotov-Ribbentrop Pact. Following the collapse of the Soviet Union, Estonia declared that all immigrants that have entered the country after 1940 are obliged to pass a language and history test before they can acquire Estonian citizenship. The regulation inadvertedly left the Russian minority in Estonia marginalized, without a clear political voice and status under the new, Estonian system.

The contentious relationship between the Estonians and Russians living in Estonia stems from the Soviet experience, while the Russian minority felt mistreated in some way. After declaring Estonia a Soviet republic, Stalin forced the small Baltic nation to become completely subordinate to Moscow. The Soviet authorities took full control of Estonia and were tasked to transform Estonia into a Soviet republic: centrally-planned economy, collectivization, and the realities of labor camps in Siberia. All of the Soviet-imposed changes have been met with grave dissatisfaction and resentment from the local Estonians, who felt oppressed under the new, imposed system. To assert their legitimacy in a nation charged with cultural and political hostility, the Russians celebrated and promoted the World War II victory. A bronze statue of a Soviet soldier was erected in the capital as a memorial for the unknown soldier in WWII. To the Estonians, however, the monument was a visual affirmation of Soviet oppression and occupation that deeply hurt their national pride. On 27 April 2007, after more than fifteen years since its independence from the USSR, the Estonian government decided to move the statue to a military graveyard in the outskirts of the city. The decision was met with outrage and retaliation from ethnic Russians, who rioted and looted downtown Tallinn. The event was ultimately a catalyst for the Internet war discussed in this article.

The Initiation. Political and ethnic tensions manifest themselves through a variety of outlets, and in the case of Estonia—through cyberspace. Staged by Russians, the cyber attack on Estonia—the depth of the incursion, the organization of its perpetrators, and the threat to Estonian national security—escalated this incident from a case of petty hacking to an Internet war with real implications for regional stability. Such brute force attacks are also known for the possibility of an Internet global fallout, as the attacks can be relayed through the global infrastructure.

On 26 April, public unrest gave way to virtual attacks on Estonia's network infrastructure, targeting government offices, news agencies, and banks. While the attack was political in nature, banks became a major target since many Estonians often rely on online banking services. Over the years, Estonia has outpaced its European counterparts in integrating the Internet in all aspects of its everyday life, becoming a truly online society. In lieu of attending traditional parent-teacher conferences, Estonian parents communicate with their children's schools and teachers online. Virtually all financial transactions are processed online. In the last elections for the Estonian parliament, over 30,000 Estonians voted from their homes, on the Internet.

In the days leading up to the attack, numerous clues pointed to a large-scale operation that was being planned online. Russian-language Internet discussion forums were abuzz with preparations for an online attack. Three days before the expected onslaught, Estonia planned to release the news of the coming strike in hopes that European media attention would oblige the EU to pressure the Kremlin to intervene, whether or not the attacks emanated from the Russian authorities. At the time, a meeting between Russian President Vladimir Putin and German Chancellor Angela Merkel, who then shared the rotating EU presidency, was fast approaching and pressure from within the EU compelled

Estonia to refrain from releasing the statement.

A cyber riot against Estonian government websites commenced at 10:00 p.m. on 26 April 2007, fueled by step-by-step instructions so simple that any Internet user could follow, complete with a preselected list of targets. The attack, whether intentional or not, coincided with the physical riots taking place in Tallinn's streets. By the next day, the attacks reached significant scale and put severe strains on Web servers, inundating the Estonian government network with malicious traffic. In the following days, more websites and mail servers, including those of banks, news outlets, and schools, became victims of the attacks.

Political and ethnic tensions manifest themselves through a variety of outlets, and in the case of Estonia—through cyberspace.

The Estonian Computer Emergency Response Team (CERT), in cooperation with local providers and volunteer networks of IT professionals in industry and government, coordinated the emergency defense program. The team was immediately involved in analyzing the severity of the incident, sending abuse reports to service providers abroad, and facilitating information exchange between the affected organizations and service providers. Though the Estonian CERT was able, to a degree, to mitigate the impact of the attacks, due to its ad hoc, unofficial status, it lacked the authority to enforce its recommendations on all parties involved.

The Unknown Attacker. Though it remains unclear whether the Russian government officially sanctioned the strike, it is undisputed that Russians were responsible. Russian-language websites, online forums, and blogs came alive with chatter about the moving of the war memorial and the subsequent cyber attacks in Estonia. Some Russian-language websites even posted messages outlining potential Estonian targets to attack and manuals for how to proceed.

The technological systems in place to trace the sources of the cyber attack and those involved provide insufficient and unreliable information. Because the protocols used to run the Internet were originally designed in an open, all-inclusive environment, information streams can easily be falsified. The allocation of Internet Protocol (IP) addresses to large areas, such as countries or regions, makes it difficult to pinpoint the exact location of a computer or a source. Moreover, the IP addresses of computers and networks can also be falsified. Finally, computers can be hacked—taken over and compromised—allowing anyone to manipulate and use them anonymously as proxies for their own attacks.

While the exact source of the attacks remains unknown, evidence suggests a highly organized assault. Not only did the cyber riot start almost simultaneously with the actual riots, fresh posts in the Russian-language blogosphere continuously appeared with new targets and instructions. These details suggest that the cyber attackers reacted to Estonian defenses. The attackers launched "botnets," online robot networks, into Estonia's IP space from the outside. Centrally-controlled Trojan horse software then transformed a network of compromised computers into a botnet. When attacks from abroad were successfully mitigated, botnets were launched from compromised computers inside Estonia.

It is evident that Russian bloggers and their followers did participate in the attacks. We cannot tell, however, who it was that inspired them. Once bloggers started reporting their small-scale attacks, more experienced players became involved. Before long, botnets were being used. The involvement of the Russian government in the affair cannot be confirmed. What raised speculation, however, is the failure—or unwillingness—of the Russian authorities to stop the cyber riot against Estonia for over three weeks after the initial attack.

Not only did the cyber riot start almost simultaneously with the actual riots, fresh posts in the Russian-language blogosphere appeared with new targets and instructions.

Crisis Response and the Internet as Critical Infrastructure. In retrospect, Estonia did not have the necessary defense mechanisms to confront a large-scale Internet assault. The incident exposes some of the structural vulnerabilities of the Estonian state and shows the importance of effective emergency response systems. Moreover, the Estonian authorities need to revise some of their former preconceptions and define the Internet as critical infrastructure, equally strategic to national security as its electricity grid and water supply.

The CERT coordinated a successful response to the unexpected cyber crisis and ultimately helped Estonia get back on its feet. The team organized an online chat room, which became a safe forum where defenders from across the geographic region and from all relevant organizations could articulate and exchange their personal anecdotes and information. The forum also provided the Estonian authorities with real-time information on attack targets and types, and communicated with foreign CERTs and the international Internet security operations community. Four CERT organizations from Germany, Finland, and Slovenia filed abuse reports documenting the incidents. Global cooperation with trusted contacts helped synchronize an effective, multilateral response.

Preventing disruptions from accidents or attacks, however, is not enough. In today's world, Internet security demands a robust response capability that can utilize defensive measures to ensure cyber, as well as civilian, order.

It is clear that computers across the world can be compromised, spoofed, and utilized in attacks. Thus, the power of one computer to impact and undermine the security of another computer, organization, or even a nation is alarming and deserves greater attention from authorities. Online attacks damage not just the intended target, but can disrupt international Internet traffic.

Recent global trends—from industrialization and urbanization to rapid diffusion of technology—make the world increasingly dependent on and vulnerable to the forces of the Internet. Though the attacks in Estonia did not hurt critical infrastructure, energy, and transportation, the incidence reveals the inherent weaknesses of the state authorities to protect their citizens and industries against analogous strikes. An Internet-staged attack on energy could easily disrupt entire supply and distribution chains, prompting severe shortages and other negative spillover effects to the entire nation. In a second, an entire city could be left without power, leaving households without electricity, streets without lights, and airports without air traffic control systems. In Estonia, however, private and business infrastructure, including banks, Internet Service Providers, and media websites, came under direct attack—making the business and private infrastructure more critical.

Personal computers on broadband connections were a neglected weakness in Estonian Internet infrastructure. Compromised personal computers launched the majority of the attacks. The challenge of protecting this infrastructure from coordinated Internet attacks, even at the level of criminal activity, has yet to be sufficiently addressed. Thus, personal computers need to be reprioritized and considered as critical infrastructure in order for appropriate defense strategies to be developed.

Internet Warfare. The political elements of the virtual attack remain complicated. Technical data has shown that one of the attacks came from an IP address allocated to the Russian government. This computer may have been involved in initiating the attacks, but could have just as easily been a spoofed address or compromised computer. This shows that manipulating technical data could be widely used for political needs and purposes. While Estonia could use the Internet war to cast criticism on the Russian government, the Russians could use it to advance their political agenda through individual computer users and networks.

In the aftermath of the attacks, many questions concerning the proper response to this new kind of warfare remain unanswered. Does an Internet attack warrant a reaction from NATO? What about the UN? Is there such a thing as a "just" Internet war, and what is a country's right to defend itself against one? As the world becomes increasingly dependent on the Internet, coordinating effective global responses to cyber attacks is critical for national security. However, international legal mechanisms and law enforcement authorities are hard-pressed to keep pace with the complexities of cyber-crime. While some politicians today often do not even recognize that the threat is plausible, denying its existence altogether, others willingly choose to neglect it.

Politics Today. The current dynamics surrounding Internet warfare—its sophisticated organization and intelligence, global scale and impact, and politicized incentives and targets—signal the beginning of a new era for global security. The attacks in Estonia ushered a quick NATO response, which—although had no discernable impact—indicated a high level of political attention for the incident. Four weeks after the events in Tallinn, the Pentagon dispatched a team to gather information about the incident. President

Bush spoke with Estonian President Toomas Hendrick Ilves on the subject in June 2007. NATO has agreed to establish research facilities to develop new ways to respond to future cyber attacks.

In the case with Estonia, the perpetrators used the Internet to both organize and execute their attack. Prominent military historian Martin van Creveld first noted several decades ago that future fighting may occur among organizations, rather than countries. Today, this has become obvious that the impact of such fighting can now be achieved at a low cost and remotely, by populations, small groups, and even individuals, not necessarily organized under any banner.

Policy Recommendations. Although authorities understand how computer attacks work and grasp their potential damaging effects, because Internet warfare is a relatively new phenomenon, there is a lack of experience and case literature on subjects ranging from strategy to tactics. For the initiator, the Internet provides an easy, low-cost, risk free method to achieve immediate, large-scale impact. Because illicit tools such as botnets exploit millions of compromised computers, security experts cannot easily find computers free of malicious software. Although the private sector may not be keen on government intervention in Internet security, firms will welcome, if not demand, state involvement once the crisis strikes their own operations.

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. Legal standards for the provable damages of cyber-crime need to be reformed since they inherently differ from physical damage. 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. Countries should create CERT authorities which are able to coordinate law enforcement and private industry on security incidents and criminal activity, while maintaining operational relationships with similar organizations world-wide. These can prove essential for future attacks, both against themselves and others nations.

Given that some countries, such as Russia and China, have lax standards for prosecuting Internet offenders, it is important that the move comes from Western nations, who should reach out and develop treaties and agreements, as well as facilitate, monitor, and enforce much faster cooperation in law enforcement. In a world of increasing political uncertainty and cyber dependency, multilateral state-led action, in cooperation with industry stakeholders, is required to help protect the national and global infrastructure, which is the Internet.