European Affairs

Cyber War I: Estonia Attacked from Russia

Kertu Ruus

Suddenly, the lights go out. Communication lines fall silent. Internet connections are lost. People venturing into the congested streets discover that banks are closed, ATMs are malfunctioning, traffic lights are jammed. Radio and TV stations cannot broadcast. The airports and train stations are shut down. Food production halts, and the water supply starts rapidly diminishing as pumps stop working. Looters are on the rampage; panic grips the public; the police cannot maintain order.

This grim picture is not the opening scene of a Hollywood fantasy, but the beginning of a cyber attack, as described by Sami Saydjari, president of Professionals for Cyber Defense, to a Congressional homeland defense subcommittee in April 2007. In vivid terms, he described how a superpower can be reduced to third-world status by a cyber take-down of a nation's electronic infrastructure. The defense expert called his description "a plausible scenario" – and one for which the United States is unprepared. Even if military computer systems are usually protected against outside interference, most civilian electronic systems remain vulnerable to a massive assault that enjoyed the sponsorship of a state.

Exactly one day after Mr. Saydjari's congressional testimony, reality took the stage in the form of a large-scale cyber assault against a nation's digital infrastructure – not against the United States but Estonia, a tech-savvy nation of 1.3 million that is a member of both NATO and the European Union. The attacks were launched from Russia, Estonia's neighbor to the east and former occupier, apparently to punish the small state for daring to relocate a Soviet-era war memorial in Tallinn, the Estonian capital.

The episode has since been dubbed the world's first cyber war, or "Cyber War I", because it was the first time that a sustained, wholesale and politically motivated e-assault was launched to wreak havoc on a country's entire digital infrastructure. Until then, "cyber security" had been limited in practice to dealing with limited and narrowly targeted hacking intrusions, often as part of a clandestine operation, to probe or disrupt military command and communications systems (including the Pentagon's). And there is nothing new about cyber criminals hacking into bank, corporate and individual computer systems to steal money or information. This wave of attacks on Estonia, however, targeted the entire civil and economic infrastructure with the aim of paralyzing the society in a country, whose high reliance on computerized networks has given it the nickname "E-stonia." (See article "E-stonia: Pioneer of Internet Innovation and e-Government" in European Affairs vol. 8 no. 1 spring 2007.)

In the event, the near-apocalyptic scenario outlined in Mr. Saydjari's testimony did not play out with all the "secondary effects" of a cyber war bringing a society to chaotic collapse. Not this time. But the three-week Cyber War I took an emergency mobilization of all Estonia's special computer-wise expertise and resources – as well as international assistance – to thwart the e-assault and defend the core of the country's extensive electronic infrastructure. At its peak, the digital "invaders" arriving by internet knocked out the Estonian parliament's e-mail system for several days, and major Estonian media and banks had to shut down access to their sites from abroad temporarily. This defense – the modern equivalent of pulling up the drawbridge to protect a medieval castle – was a temporary stratagem that allowed time for counterattack as the ultimate defense.

Learning some lessons, Western countries have now taken initial steps to put in place overdue accords defining cyber attacks as a possible act of war, building up more robust defenses and agreeing on protocols for allied cooperation. A key initiative has been the creation of the NATO "center of excellence for cyber defense" joining the list of alliance facilities that develop best practices for special kinds of warfare. This one will be located in Estonia, with other NATO countries already committing to participate.

The attack on Estonia's internet systems began in the hours before midnight on April 26, 2007. Estonian-Russian relations had been brewing with bitter tensions for weeks, and that morning rioting had erupted in Tallinn, the country's historic capital on the Baltic Sea. The man who started Cyber War I was not a Russian rioter or hacker, but a bronze statue in the old city center – the Unknown Soldier memorial erected in 1947 by the Soviets and maintained during their 50-year occupation of Estonia as homage to the Soviet army for "liberating" Estonia at the end of World War II. A symbol of foreign occupation, it was never popular: Estonians dubbed it the Unknown Rapist. It was a gathering place for Red Army soldiers and their compatriots in the 400,000-strong minority community of ethnic Russians, sometimes for boisterous occasions celebrating Soviet holidays. But over the decades, Estonians tolerated the downtown monument on the grounds that the Russian community also needed a place to commemorate their fallen.

But in the early months of 2007, as Moscow started becoming more combative toward the EU, notably over gas supplies, Tallinn's Unknown Soldier started to become a focal point for anti-Estonia activists – often angry and violent. Alarmed by the trend, the Estonian government decided that a military cemetery would be a more appropriate place to memorialize the Red Army dead. After extensive public debate, the statue was relocated there at dawn on April 27th.

The reaction was swift. In Tallinn, protesters took to the streets. Rioting continued for two days. Shops were looted, cars burned. Molotov cocktails flew. Tear gas and water canons were deployed. One person died from a stab wound, many were injured and hundreds were arrested. Meanwhile in Moscow the Estonian embassy was besieged by thuggish Russian activist groups, who blockaded the building for days. The street violence had no political precedent in Estonia: during the country's elegantly orchestrated march to independence in defiance of the Soviet Union in the 1980's and 90's, not a drop of blood was spilled. The situation in Tallinn was often tense, but Estonia's revolution and transition were bloodless.

Now, as the rioting began to subside, cyber attacks escalated. For days, Russian-language web forums had lambasted Estonia for relocating the Unknown Soldier, with managers of these websites inciting "patriots" to protect Mother Russia from the "F--cking Estonian Fascists." (Interestingly, national polls show that Russians consider tiny Estonia as the leading threat to their security.) Calling for vengeance, the Russian websites advocated a strategy for destroying the e- systems that have become a vaunted success as the arteries of government and business in Estonia. This infrastructure could be shut down by overloading them with unprecedented volumes of traffic, the Russian websites said, offering directions on how to organize and launch this type of cyber attack, technically known as a "denial of service" attack. In this case, it was also a "distributed denial of service" attack because the electronic invaders took control of many other computers to join and reinforce the assault and add to the paralyzing burden of millions of incoming messages.

In retrospect, Estonia's Ministry of Defense now can reconstruct the assault as a two-phase offensive. For the first few days, the attackers – "hactivists" – were engaged in amateurish psychological warfare with propagandistic goals. Hacking into the website of the political party that leads Estonia's coalition government, they posted a fake "letter of apology" there from Prime Minister Andrus Ansip for moving the statue. Any "collateral damage" to Estonia's e-systems was temporary and manageable.

Not so in the second phase in which cyber-attack specialists joined the fray and escalated the attacks into a full-scale (and apparently well-financed) campaign. The aim was to overload Estonia's computer servers with massive volumes of message traffic causing them to crash. The attacks in this period were highly sophisticated, with the perpetrators deploying "botnets" – software robots that hijack unwitting "zombie" computers from around the world, link them together in large networks and program the network to bombard the targeted e-system with millions of fake messages. Incredibly, it is estimated that a million computers were hijacked and mobilized globally for this distributed denial of service onslaught on the servers of a country of 1.3 million inhabitants. At their peak, the botnets were barraging Estonia's computer systems with one thousand times their normal rate of incoming e-mail traffic. The messages were coming from every corner of the globe including China, Peru, the U.S. and Egypt. In fact, traffic was directed by Russian "botherders" who had manipulated tens of thousands of unsuspecting zombie computers and commanded them to clog Estonia's servers and bring down the system. Chronicling the attack, a story in the authoritative U.S. techie magazine Wired – entitled "Hackers Take Down Europe's Most Wired Country" – made the point that such elaborate attacks require not only highly skilled and quick-response expertise, but also considerable funds. In this case, the cyber attackers set up a PayPal account to raise money for hiring botnets, according to Gadi Evron, founder of Israel's Computer Emergency Response Team (CERT). He flew to Estonia at the outbreak of the attacks and spent four days there monitoring the operations.

The battle to thwart Russia's attacks was led by a former policeman, Hillar Aarelaid, the director of Estonia's CERT, who had been combating cyber-crime for over ten years when this battle erupted in April. Throughout, he was at his CERT command post every day at dawn surveying the country's IT systems to be sure they were operating before other citizens arrived in their offices. In the battle, Estonia had several critical assets. One was a small pool of information-technology friends from both the private and government sectors who worked closely together throughout the three-week battle. For years they had made up a tight social network, frequenting the same pubs and family saunas. In the crisis, they amounted to a team of friends comprising Estonia's leading cyber-security experts from the Internet service providers, media, banks and government agencies. This talent pool fused into an informal rapid-reaction force to counter the attacks: If someone had to be dragged from bed in the middle of the night to help, there were no second thoughts.

This ad hoc rapid-response unit made a strong impression on Gadi Evron, the Israeli specialist. As he later remarked, "Estonia is unique and lucky to have so many IT specialists who are friends, who work for banks and the government; and who talk to each other. The information sharing is unbelievably open."

This social IT network of Estonians was still insufficient to beat back the attacks from Russia. Beyond increasing server capacity and blocking incoming message traffic (in effect restricting access to Estonian portals from abroad), there was little that could be done in the early stage. CERT reached beyond Estonia's borders to tap additional support and expertise from contacts in Finland, Germany, Slovenia and elsewhere. NATO sent an observer.

As the campaign unfolded, Estonia's CERT team, with the help of international experts, designed and implemented a three-pronged strategic response: quickly bolster the country's server capacity ; find ways to electronically distinguish authentic e-mail traffic from zombie "attack traffic" and prevent it from reaching Estonia's servers; go on the offensive by locating and neutralizing the bots and zombies.

For this third and crucial prong, counterattacking the assailants, decisive support came from an elite international cadre of the top, most trusted techies in the internet system of governance. Some 13 individuals, known as the Vetted, are authorized by the world's largest ISPs (Internet Service Providers) to identify and remove rogue computers from the global Internet system. They are the ones in charge of the world's 13 root DNS (Domain Name System) servers, which direct global Internet traffic. By some almost unbelievable coincidence, three of the Vetted happened to be attending a meeting in Tallinn when the attacks broke.

As recounted in Wired, once contacted by Aarelaid, the three Vetted (two Swedes and an American) joined CERT headquarters late one night to monitor and screen the waves of incoming traffic in order to pinpoint the attacking rogue computers. Once an attacking computer's address was identified, the Vetted asked network operators throughout the world to block its IP (Internet Protocol) – the data link to the internet – at the source. Working through the night, the newly-augmented CERT team had thwarted hundreds of thousands of zombie computers by daybreak, taking so many rogue computers off line that traffic had dropped to nearly normal levels. The tide of Cyber War I had changed.

The casualties of the three-week assault were, in the end, surprisingly modest, temporary and few. The parliament's e-mail system was indeed inoperable for four days; the customers of the country's two largest banks were unable to access their accounts for a few hours; the main Estonian news portals were disrupted when media, including the largest daily paper, Postimees, had to temporarily shut down access to their sites from abroad. Otherwise, little changed in the rhythm of this country where 97 percent of all bank transactions are conducted online and where 60 percent of the population uses the Internet daily. Although the pace was often frenzied in CERT's headquarters during these weeks, "most ordinary people noticed nothing," Aarelaid later told Äripäev, Estonia's leading business daily.

An American specialist agrees on the modest casualty assessment: according to Jim Lewis, senior fellow at the Center for Strategic and International Studies (CSIS) in Washington, the attack on Estonia amounted to "blocking the highways and pounding on doors to make a political point," as opposed to a truly damaging offensive. "This was a display: the attackers tipped their hand," he says. Conceivably, the attackers were seeking to probe Estonia's electronic defenses for unknown future purposes.

Experts, including Aarelaid, credit the relatively light toll largely to the fact that Estonia, while appearing vulnerable because of its high dependence on e-systems and the Internet, has also invested in protecting the system. When the government made preparations for on-line national elections in 2005, which was a global first, it developed both technical expertise and sophisticated defense mechanisms to protect the elections from fraud and intrusion. Those proved useful during the attacks in 2007.

The attacks on Estonia served as a wake-up call to military and security circles in NATO nations on both sides of the Atlantic and focused attention on the need to answer some tricky questions. What defines a cyber war? What distinguishes a cyber attack and a cyber war from cyber terrorism? If an attack cannot be traced to a government, what will be the response? What "deterrence" tactics might discourage cyber-aggressors?

A prime question is: at what point does an attack warrant a NATO response on the basis that an attack on one is an attack on all? The NATO treaty protects its members against a territorial intrusion, yet the era of cyber war and electronic intrusion represents a threat akin to traditional warfare that is of a new, still-developing nature. In an interview with the New York Times, Estonia's Defense Minister Jaak Aaviksoo observed that a cyber assault intended to cut a state off from the world "can effectively be compared to when your ports are shut to the sea" – a naval blockade, which has long been regarded as an act of war. The modest casualties in Estonia's cyber war notwithstanding, there is little disagreement that a large scale and coordinated government-sponsored cyber attack, clandestine or otherwise, has the potential to cripple the targeted country's capacity to function for extended periods.

"The first battle in the wars of the future will be over the control of cyber-space," according to Dr. Lani Kass, a special assistant to the U.S. Air Force chief of staff, who spoke on the threat four months after the Estonia episode at the Air Force Association's Air and Space Conference and Technology Exposition. "If we don't dominate cyberspace, we won't be able to dominate air, space, land or sea domains," she noted. CSIS' Lewis adds that, as things stand, the advantage lies with the attacker. To bolster defenses, he says, "countries must pay more attention and spend a little more."

Moreover cyber war may be the wave of the future as a tempting tool to subdue "enemies of the state." In Russia, opposition parties claim that there is a designated unit of specialists in the FSB, the successor to the KGB, that specializes in coordinating Internet campaigns against those the authorities consider a threat. In fact, some of the computers involved in the attack on Estonia also turned up in domestic web attacks. In addition to the recent attacks against Estonia, the Russians have waged cyber attacks to disrupt breakaway forces in Chechnya (as has the U.S. in its war against terrorism: see David Ignatius' fictional but well-informed recent thriller, Body of Lies.)

In Washington, the Bush administration seems to have gotten religion on defense against cyber war. In the weeks after the attacks on Estonia, Defense Secretary Robert Gates raised the issue at a June 2007 ministerial meeting of NATO, urging the allies to develop contingency plans for cyber attacks. A key question, he reiterated, is some determination, some definition, of what constitutes an attack that triggers collective defense under NATO's Article 5.

Stressing the need for a conceptual framework, Estonia's Defense Minister Jaak Aaviksoo has stated that "the EU and NATO need to work out a common legal basis to deal with cyber attacks. For example, we have to agree on how to tackle different levels of criminal cyber activities, depending on whether we are dealing with vandalism, cyber-terror or cyber war."

While hoping for movement toward international norms on these threats, Estonian officials maintain that such an electronic assault already constitutes an act of terrorism under existing EU law. The EU defines terrorism as any action liable to seriously damage a country and committed with the aim of intimidating a population; or unduly compelling a government to perform or

abstain from performing any act; or seriously destabilizing or destroying the fundamental political, constitutional, economic or social structures of a country.

Estonia, with its special experience in the ways of cyber war, seems to be taking a lead in developing defensive strategies. It has developed its own national action plan against cyber crime, and now NATO has designated Estonia to host NATO's "cyber heart" – a cooperative cyber-defense research and strategy center located at Estonia's Training and Development Centre of the Defense Forces Communication and Information Systems (SIVAK). Its international staff is expected to rise to about 30 in 2008 as the center goes into full swing, with four other European allies committed to joining: Germany, Italy, Spain and Latvia. The U.S. is also taking part and has already posted a representative to Tallinn.

Even when NATO manages to sort out the definitions and the Article 5 issue, there are other challenges. Can NATO help identify, hunt down and prosecute a cyber criminal when the offender may be a state, or a state-sponsored cyber warrior or a freelancing cyber hacker? "The Internet is perfect for plausible deniability," notes the Israeli specialist, Gadi Evron. The very nature of cyber war offers ample opportunities for an attacker to disguise his involvement: in practical terms, cyber attacks raise some of the same problems that confront governments trying to track down and punish – or, equally, to deter – the sponsors of bloody non-cyber terrorist acts.

Estonia's recent efforts to identify their attackers are instructive. In the early days of the assault, Estonia's Foreign Minister Urmas Paet issued a statement claiming that cyber terrorist attacks "have been made from IP addresses of concrete computers and individuals from Russian government organs including the administration of the President of the Russian Federation." Adding to the intrigue, senior Estonian officials privately claim that several of the attacking computers were traced directly to the Kremlin.

Russia denied the allegation and warned Estonia against making further charges without proof. The Russians have a point: the IP addresses which the Estonian team tracked down to the Putin administration may well have been hijacked "zombie" computers. Though there are obvious reasons to suspect Russian government involvement, there is no way to be certain – a classic case of "plausible deniability."

Besides denying any culpability, the Russian government further complicated the effort to track down the cyber criminals by refusing to cooperate with the Estonian authorities to investigate the case. As a number of attackers within the jurisdiction of the Russian Federation were identified, the Estonian State Prosecutor made a formal investigative assistance request, which Moscow rejected, alleging that procedural problems prevented cooperation.

When a host government fails to cooperate in an investigation of a cyber attack, the victim's options are limited. One can easily imagine that this pattern of deniability and stonewalling will complicate future efforts to track and prosecute cyber criminals in any number of countries.

In sum, the cyber war against Estonia offers an unsettling glimpse of the potential chaos and devastation that could befall nations whose leaders fail to anticipate and prepare for the cyber attacks of the future. Incidentally, too, the events offer a sobering reminder of the strong-arm methods that seem to enjoy increasing sway in Russia.

The most profound consequence of Cyber War I, however, may well be that the attackers, perhaps inadvertently, launched an awareness-raising campaign in the West, delivering a wake-up call to individual governments and international organizations alike about the vulnerabilities of their vital civilian electronic infrastructure.

Kertu Ruus *is the Washington-based U.S. bureau chief and a member of the editorial board of the daily Äripäev, the largest business publication in Estonia.*

This article was published in European Affairs: Volume number 9, Issue number 1-2 in the Winter/Spring of 2008.