Erin Dian Dumbacher

Visit " Governing Security in a Networked World " to see in-depth video interviews with top thinkers on cybersecurity .

In the spring of 2007, Estonia became the first nation to face a coordinated, nationwide cyberattack when a series of electronic bombardments struck down media, telecommunications, government and banking websites. Digital traffic from servers as far away as Peru, Vietnam and the United States flooded Estonian websites, drowning them in superfluous data. The attack knocked telephone exchanges offline for more than an hour, jeopardizing emergency services. It knocked out media and government portals, leaving citizens in an information vacuum. Beginning April 29, three waves of attacks during a two week period severely disrupted the ordinary tasks that fuel modern economies -- shopping, pumping gas, withdrawing cash from automatic teller machines. A significant act of cyberterrorism posed an economic and political threat in a way no modern economy had previously experienced.

The onslaught against Estonian websites began after two days of rioting in the capital, Tallinn, spurred by the government's removal of a Soviet-era statue honoring deaths in World War II. By the time officials cleared the streets of shattered glass and protesters, the dispute had moved online.

Though primitive by today's standards, the distributed denial-of-service attacks on Estonia highlighted the central dilemma of online attacks -- attributing the assault to the individuals or governments behind them. While attribution is elusive -- skilled attackers typically hijack foreign servers to perpetrate their crimes -- it is widely believed that Russia funded and led the execution of the attacks against its western neighbor. The architecture of the Internet allowed networks of bots, called botnets, to direct millions of packets to the servers of the Estonian targets, overloading and rendering them inaccessible to visitors.

"It's a new form of public-private partnership," warned Estonian President Toomas Hendrik Ilves in an April interview with *Nextgov*. "It requires massive numbers of computers. There are organized crime rings and they do this by length of time, but you have to have someone willing to pay for it -- that's where the public side of the public-private partnership comes in."

Had the small Baltic nation not been one of the most wired countries in the world, such an attack might have been a blip on the screen of public awareness. In the two decades since breaking away from the former Soviet Union, Estonia built its new democratic society around Web-based services. Estonians were among the first to conduct elections online and today they perform 98 percent of their banking online. For the nation that spawned the global telecommunications phenomenon known as Skype, the 2007 attacks were a watershed moment. Estonia's experience and subsequent actions continue to offer lessons for security managers who face more advanced threats today.

Professional networks are critical

The informal relationships among technology professionals built through old-fashioned networking were key to government and private sector responses to the crisis in 2007. Estonia's two-person computer emergency response team recruited help, calling on national and foreign experts. Swedes and Americans especially aided the response efforts by halting Internet traffic before it reached Estonia. The government also turned to the local, private specialists who had helped set up the country's electronic-voting security system.

The professional network of technologists is small, yet formal mechanisms for quick and effective coordination did not exist. Estonian officials are now establishing policies and procedures to activate this network as needed and have recruited a volunteer army of IT professionals from public and private organizations -- a National Guard for cyberdefense. Volunteers train on weekends for emergencies, while employers gain a more experienced

workforce. Internationally, Estonia advocates for more stringent cybercrime regimes and clear cybersecurity policies among NATO allies. What is the lesson for U.S. leadership? Use meaningful, project-based collaboration to connect with colleagues across agencies and in the private sector.

Go beyond 'partnership'

Infiltrators do not respect national borders or distinctions between public and private infrastructure. An adequate response to a cyberattack requires coordination among various organizations and individuals in the government and the private sector.

Working with the private sector in Estonia required more than just regulation. While regulators encouraged private sector feedback and information sharing, officials found that cooperation needed to be institutionalized; voluntary associations were insufficient to create the kinds of relationships necessary to coordinate an effective cyber response. Large organizations had the resources to maintain their own systems; small and medium-size enterprises were vulnerable. All needed incentives to share the details of their breaches.

The challenge is global because the networks are global. While NATO and other international bodies are recognizing and acting on the need for more effective partnerships, "I think where we really need to do work is redefining the boundaries between the government [and the] private sector," Ilves said.

Acknowledge the international dimension

Today, the centerpiece of Estonia's cybersecurity strategy is engagement with foreign partners' networks and intelligence operations. Estonia has consciously enhanced its partnership with the FBI and it played a central role in standing up the NATO Cooperative Cyber Defense Centre of Excellence in Tallinn, which stages attack scenarios and encourages members to share best practices. Linnar Viik, Estonia's technology guru, is a regular participant in cyber-related efforts by the United Nations and the Estonian government advocates signatories to the Council of Europe Convention on Cybercrime. The United States signed on in 2006 and most European countries have joined. Russia and China have not.

Get ahead of the threat

Without official processes in 2007, Estonian site managers first tried the "whack-a-mole" approach, trying to defeat each wave of traffic separately. As the onslaught continued and the origins of the traffic came from a diverse set of servers around the world, managers shut off all inflow from abroad. The liberty to shut off all foreign traffic is one the U.S. does not have; restricting access could severely damage the global economy.

The Obama administration has been consumed with a series of economic and political crises since taking office, with the whack-a-mole moniker attributed to its policy in the Middle East, the economy and more. Estonian policymakers had the benefit of a crisis to form a comprehensive strategy and to advise the public how to prepare for and retaliate against upcoming attacks. U.S. private and public networks cannot afford to be unprepared.

Erin Dian Dumbacher is the associate director of research at the Government Business Council, the research division of the Government Executive Media Group, to which Nextgov belongs. She studied technology development and cybersecurity as a 2009-2010 Fulbright Fellow in Estonia. This week, GBC launched a month-long video series on cybersecurity featuring in-depth interviews with top policy and academic experts. To see the series, "Governing Security in a Networked World," visit http://www.nextgov.com/governing-security-in-a-networked-world/ ".

Original article on the Newtgov homepage .