New Weapons: Keyboard and Mouse

Cybersecurity cooperation is key to defeating hackers

The Internet continues to grow as an essential, daily tool for billions of people in personal, corporate and government arenas. Protection of confidential online information, also known as cybersecurity, therefore also grows in importance. Cybersecurity defends against illegal use of the Internet, corruption or disruption of computer networks and software, hacking and espionage. The global, borderless nature of the Internet calls for legal, political and private cooperation around the world, as cyber attacks are rising in frequency and severity, with hundreds of thousands of attacks launched daily at the cost of billions of euros. Our growing dependence on cyberspace makes cyber security a high priority that's appearing atop policymaker agendas.

Cyber threats and espionage are two of the most pressing issues in the world today. Cybercrime is one of the fastest growing and most lucrative aspects of illegal Internet use. Proceeds from identity theft have even outpaced those from illegal drugs, according to Deutsche Welle.

One of the most well-known cyber attacks took place in Estonia in 2007, resulting in denial of service on all government and banking sites for three weeks. Customers received error messages when attempting to make a transaction. As one of the most wired countries in Europe, this small Baltic nation was particularly disrupted, as Estonians conduct 90 percent of their banking online. They pioneered development in paperless e-government and pay for parking with cell phone Internet hookups. After this attack, NATO and the European Union rushed information technology specialists to Estonia to assist in the recovery.

As countries further embrace Internet use, the risk of attacks increases. Task forces, summits and conferences on this subject have proliferated since the Estonia attack. Pooling resources, more than a dozen European organizations have enacted policies or held discussions, including the European Commission, NATO and the U.N. However, despite the efforts of highly intelligent security professionals working to secure networks in government, military and private industry, it is difficult to defeat these hackers that work obsessively to destroy computer networks.

Cyber hacking attracts extremists and spies because it can be done anonymously, safely and cheaply. Attacks vary from stealthy thefts on the Internet to advanced, persistent threats. Infected memory sticks allow criminals to steal documents and e-mails from computers. Traditional spies risk their lives to smuggle documents, but those who attempt theft in the cyber world face far less serious penalties. Current cybercrime laws do not appear to deter criminals. For example, NATO headquarters is attacked at least 100 times a day, NATO Secretary General Anders Fogh Rasmussen has said. The Center for Strategic & International Studies mentions several international hurdles to defeating cybercrime: "Disagreement over what constitutes a crime; inadequate, uneven or absent authorities for governments to investigate and prosecute cybercrime; and procedures for international cooperation more attuned to the age of sail than to the Internet."

Despite preventative efforts, some fear what the mass disruption resulting from a substantial cyber attack might entail. The *EUobserver* describes it this way: "The EU's 27 countries would wake up to find electricity power stations shut down; communication by phone and Internet disabled; air, rail and road transport impossible; stock exchanges and day-to-day bank transactions frozen; crucial data in government and financial institutions scrambled and military units at home and abroad cut off from central command or sent fake orders." Economic damage and data loss could, therefore, last for years.

Countries attacking countries

The Guardian reported in May 2010 that "[cyber] attacks launched by countries against other countries are causing the greatest concern." Recent examples include:

- In June 2010, China was accused of wholesale espionage, attacking computers used by U.S. defense contractors and stealing classified details of an F-35 fighter, the BBC reported. In addition, in 2009, the Chinese targeted Google and another handful of information technology, or IT, companies.
- North Korea was blamed for a massive cyber attack on the United States and South Korea in July 2009, according to Reuters. More than two dozen Internet sites were attacked, including those affiliated with the NASDAQ stock exchange; the White House;

Melissa Hathaway, acting senior director for cyberspace for the U.S. National Security and Homeland Security Councils, speaks at a conference in Estonia in June 2010. The conference tackled the issue of cyber conflict.

AGENCE FRANCE-PRESSE

the State, Treasury and Transportation departments; the Secret Service; and the Federal Trade Commission. Internet service providers in South Korea distributed a computer vaccine to combat the virus. In addition, a newspaper and two major lender sites in South Korea were affected, according to a *Telegraph* article in July 2009.

- In 2008, the Georgian government accused Russia of orchestrating "denial of service" assaults against Georgian websites starting just one day before the Georgian and Russian militaries began fighting over South Ossetia.

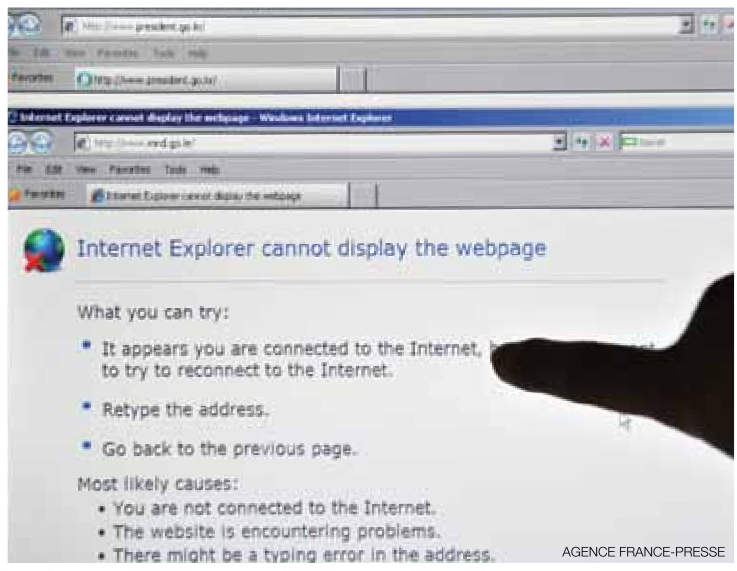
Reports suggest China continues to invest in its network operations and represents a cyber espionage threat. "The fact that so much vital personal and organizational information, as well as financial transactions and operating systems are now placed in the cyber domain means a number of highly valuable targets are available for a range of state and non-state actors," *Jane's* intelligence clearinghouse said. In January 2010, Google announced that persistent cyber attacks emanating possibly from China may force the company to discontinue its Chinese search engine, google.cn.

Cooperation is critical

Cooperation and information sharing are critical to prevent further attacks. The United States, Russia and China, along with 15 other nations, agreed for the first time in July 2010 to work on

Flowers adorn a Google logo in front of the company's China headquarters. Google, the world's most popular search engine, threatened to shut down its Chinese-language google.cn search engine in 2010 over censorship and attacks from China.

THE ASSOCIATED PRESS



Internet Explorer cannot display the webpage - Windows Internet Explorer

Internet Explorer cannot display the webpage

What you can try:

- It appears you are connected to the Internet,
  to try to reconnect to the Internet.
- Retype the address.
- Go back to the previous page.

Most likely causes:

- You are not connected to the Internet.
- The website is encountering problems.
- There might be a typing error in the address.

AGENCE FRANCE-PRESSE

A suspected North Korean cyber attack shut down the home pages of the South Korean president and Defense Ministry in July 2009.

reducing the threat of attacks on each other's networks. One of the recommendations resulting from this agreement was that the "U.N. create norms of accepted behavior in cyberspace, exchange information on national legislation and cybersecurity strategies, and strengthen the capacity of less developed countries to protect their computer systems," *The Washington Post* reported. Other nations participating in the agreement are Britain, France, Germany, Estonia, Belarus, Brazil, India, Italy, Israel, Qatar, South Korea and South Africa.

NATO addressed cyber attacks in its Strategic Concept adopted by member nations in November 2010. The Strategic Concept affirms that cyber attacks are an increasing, eminent threat. "Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability," the document states. It further acknowledges that "foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks." Responding to cybersecurity threats is not optional for NATO, Ashley J. Tellis of the international think tank Carnegie Europe argued in a debate involving NATO, Carnegie Europe and government officials. She contends that cyber threats, as well as climate change, terrorism, and proliferation of WMD "are at the core of fulfilling its obligations to the security of its member states." NATO also announced the creation of an Emerging Security Challenges Division, which includes cyber defense as one of its initiatives.

Experts agree that the private sector must participate in cybersecurity at the same level as government and militaries in order to create comprehensive effective cyber protection. "Private businesses already are investing in this area simply to protect themselves, therefore partnering with them is a good idea and pools resources," *Jane's* reported in January 2010.

A unified policy will benefit the world, but creates a steep road ahead. This policy will need to include: jurisdiction; a universal definition of cybercrime; determining the level of cyber attack (e.g., monetary damages, deaths, length of disruption); extradition; language barriers; public education; and education of police, legal and judicial officials on technical subject matter.

The Internet is a prime example of how new opportunities can create new challenges. Looking to the future, cyber attacks are not likely to cease, but the response needs to improve, according to IT security experts. Pre-empting attacks will be critical: The world must combine resources to address cyber attacks and prevent exciting technologies from becoming liabilities.

The next issue of *per Concordiam*, due out in the summer of 2011, will address the theme of cybersecurity in greater detail. □