Getting Serious about Cyber Security

The Internet poses a geopolitical threat to Europe and its neighbors

By *per Concordiam* Staff

One way to gauge the relative importance that different world organizations place on cyber security is to compare the paths taken by NATO and the European Union. NATO sponsors a Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia in recognition of a well-publicized attack on that country's financial system in 2007. The European Union established the European Cybercrime Centre (EC3), published an official European Cyber Security Strategy and proposes data privacy legislation. Collectively, NATO and the EU are working to prevent and disrupt cyber attacks by dismantling large cybercrime networks, creating a standard for cybercrime reporting and protecting customers' personal information. With the CCDCOE providing training and capacity building, and the EU providing civilian applications, they are making the Internet a safer place for Europeans.

An interior view of the new European Cybercrime Centre at Europol headquarters in the Netherlands, which opened officially in January 2013.

Interpol estimates that about a million people in Europe are victimized daily by cyber crime for an annual monetary loss of 750 billion euros. Those figures inspired the European Commission to create the EC3 in The Hague in January 2013. The centre targets organized crime networks, by which a large portion of cybercrime is committed, and those who target critical infrastruture or IT networks. Plans call for more than 50 investigators with a budget of 3.6 billion euros. The commission views the new Europol division mostly as a bulwark against the economic and social costs of online criminality, including identity theft, e-crime and the sexual exploitation of children. "This is a good day for Europe," Cecilia Malmström, EU Home Affairs Commissioner, said at the opening of the Centre in January 2013. "…we send a signal to cyber criminals that we will go after them. And by 'we' I mean 27 member states together with the EU institutions, as well as industry, academia and civil society. Never before has the EU responded in such a strong way."

The European Cyber Security Strategy, likewise, applies a multidisciplinary approach. Released in February 2013, it mandates that each state designate a computer emergency response team for cyber emergencies and reporting of cybercrimes, and bolsters public/private sector cooperation. "The more people rely on the Internet the more people rely on it to be secure. A secure internet protects our freedoms and our ability to do business. It's time to take a coordinated action—the cost of not acting is much higher than the cost of acting," European Commission Vice President Neelie Kroes said of the strategy in February 2013.

The EU's cyber protection efforts also include a unified European data protection law to replace 27 different national laws governing cyberspace. New privacy rights, backed by stiff fines for violators, would include a "right of portability" (marketers would be required to get a customer's consent before transferring data) and a "right to be forgotten" (customers could wipe user data clean from websites they have visited). The rules will bind both EU companies and foreign companies that process the data of EU citizens or serve the EU market.

Although welcome, limiting abuses in the realms of social media and e-commerce is viewed as insufficient to an increasing number of observers who fear rogue operators on the Internet pose a larger, geo-political threat. That recognition was behind the establishment of the NATO centre of excellence in Tallinn, Estonia, in 2008, followed by the creation of a U.S. Military Cyber Command in 2010.

Some military observers view cyber attacks, particularly those they suspect are sponsored by governments, as Internet versions of reconnaissance to scout out a geo-political rival's defenses. With that in mind, cyber preparedness "exercises" are becoming more routine and include participation by the private sector. "The consequences of a well planned, well executed attack against our digital infrastructure could be catastrophic," then-British Armed Forces Minister Nick Harvey told the *Guardian* newspaper in 2011. And sometimes the best defense is a good offense. According to a story in Britain's *Daily Telegraph*, al-Qaida's online magazine was hacked in 2011 and a manual for bomb-making replaced by cake recipes.

Independent and state-sponsored hackers increased their presence on the international scene in 2012, damaging economies and business operations. Computer security company Symantec estimates the cost of global cyber crime at $114 billion (87.1 billion euros) annually with another $274 billion (209.4 billion euros) in time lost due to down time. In a speech before the American Enterprise Institute in July 2012, Gen. Keith Alexander, commander of the U.S. Cyber Command and Director of the National Security Agency, labeled cyber crime "the greatest transfer of wealth in history."

In August, the giant Saudi oil company Aramco lost much of its corporate data to a computer virus. Multinational defense contractor Lockheed Martin Corp. reported "persistent" attacks on its networks throughout the year. Financial institutions, including Visa, MasterCard and the New York Stock Exchange, have been targets as well. U.S. and NATO military computers are not immune either. The virus dubbed "Red October" attacked "files encrypted with software used by several entities from the European Union to NATO," according to a January 2013 Agence France-Presse article.

Some have compared cyber attacks to the nuclear standoff of the last century. As was the case with nuclear arms, fear of retaliation and escalation might prevent governments from wielding the "cyber weapon." Nevertheless, cyber disruptions will likely play a role in future conflicts. According to Gen. Alexander, cyber attacks have thus far been primarily "disruptive," but he foresees "destructive" attacks that could disable power grids or knock our air-traffic control systems. Gen. Alexander urged NATO Allies to prepare a good defense that would include a system of real-time information sharing between the private sector, especially critical infrastructure industries, and government security agencies. An important component of such a system would be protecting civil liberties and privacy.

Said *The Economist*: "After land, sea, air and space, cyberspace is now the fifth dimension of warfare. Could a country launch a crippling attack from cyberspace, say to knock out the electricity grid of a rival state, or snarl up the logistical chain of its armed forces? The answer is: maybe." □