

E u r o p o l

From the earliest of days, humans have warred against and stolen from each other, with the tools evolving over time from sticks and stones, to arrows and spears, to guns and bombs. Physical weaponry is familiar and readily recognizable. But today, algorithms and computer code have moved to the forefront. Cyberspace has become a new battlefield, one that often involves targets such as financial systems and communications networks.

[illegible]

A major challenge in fighting cybercrime is to even concretely define it and measure the amount of cybercrime taking place. Estimates of how much cybercrime costs companies and individuals vary widely. For example, some experts indicate that cybercrime has cost €2 billion in the United Kingdom, but other estimates put the total global effect of cybercrime at hundreds of billions of euros. Not only that, but cybercrime is also a global problem, and countries have attempted many different strategies to fight it with a standard approach. The EC3 will help to standardize approaches to better counteract European cybercrime, and will help set guidelines regarding what incidents constitute cybercrime.

235

and contracted staff. Still, concerns remain as to whether the current level of funding will be enough to keep pace with the projected increase in cybercrime over this period.

The EC3 describes its operations as having five main functions. First is data fusion, which involves gathering and processing information on cybercrime. The EC3 hopes to function as a central repository for statistics on cybercrime and its apprehension. Its second function will be cybercrime prevention operations, including conducting cybercrime investigations within individual EU states or facilitating joint investigations across multiple EU states. The third major function of the EC3 will be developing strategies for fighting cybercrime, analyzing crime trends, and forecasting future trends in cybercrime. The fourth function will be research and development as well as training of law enforcement agencies in the skills required to effectively investigate and combat cybercrime. The organization will also educate judges and prosecutors on cybercrime. Lastly, the EC3 will conduct outreach, working with the private sector, academia, and society at large to better handle cybercrime.

The majority of credit card numbers used in cybercrime in the EU have historically originated from United States data breaches, so a major focus of the EC3 has been preventing card-not-present (CNP) fraud. Europol reports that organized crime makes €1.5 billion from credit card fraud, 900 million of which originate from CNP fraud. As technological infrastructure improves in developing nations, it is expected that incidences of online credit card fraud originating in Africa and other similar countries will increase. The EC3 will need to be prepared for this type of cybercrime becoming more prevalent.

The early results of the EC3 have been positive. In 2013, it took down the largest ransomware cybercrime network in Russia, Operation Ransom, which spanned 33 countries, including 22 in the EU. Operation Ransom infected computers with police ransomware, which is a type of malware that blocks a computer completely and warns the user that they have visited illegal websites, such as child pornography, and requests payment of a fine to unblock it. The leader of the ring was arrested in Dubai by Spanish police and Europol along with at least ten more members of the group. In September 2013, in an operation code-named "Operation Ransom II," EC3 and Spanish police arrested two Ukrainian cybercriminals who sold access to a botnet with over 21,000 compromised servers located in 80 different countries. They also operated a sophisticated money laundering scheme that processed around €10,000 a day through various electronic payment systems and virtual currencies. These two investigations were part of EC3's "Focal Point Cyborg," which assisted in a total of 19 cybercrime operations in the EC3's first year of existence.

As part of its "Focal Point Terminal" division, the EC3 busted an Asian criminal network responsible for the theft of 15,000 credit card numbers and for conducting illegal Internet transactions and purchases of airline tickets. In July, the EC3 held a 'day of action' to target criminals using stolen credit cards to buy airline tickets as part of a different ring. Europol and individual law enforcement officers worked in concert in each country to make the arrests, which are expected to yield further links to other criminal organizations. A third area, "Focal Point Twins," focused on nine sophisticated online child sexual exploitation rings in EC3's first year.

The EC3 is currently focused on fighting “cybercrime-as-a-service.” Experienced cybercriminals are selling programs and services that buyers can use to commit cybercrime without the same knowledge of criminal techniques. When cybercrime is committed outside of the EU’s jurisdiction, it is more difficult to police, so many skilled cybercriminals within EU borders have taken to cybercrime-as-a-service to reduce their risk, allowing others to execute the cybercrime instead. Criminals are also increasingly making use of legitimate tools to stay anonymous on the Web, such as encryption techniques, virtual currencies like Bitcoin, anonymization services such as Tor which are used to navigate areas on the Web known as the “Darknet,” private networks where connections are made without sharing IP addresses.

Troels Oerting, head of the EC3, noted that although these obstacles are daunting, worldwide cybercrime is driven by a small number of talented programmers, and that focusing on these “top-level” criminals is the best way to combat cybercrime going forward. To that end, EC3 has launched a cybercrime task force in tandem with other law enforcement agencies called the Joint Cybercrime Action Task Force, which will focus on developing strategies for handling newer cybercrime techniques, pursuing the most dangerous cybercriminals, and further improving the flow of data between law enforcement agencies across borders. In November 2014, the EC3 demonstrated its ability to shut down sites on the Darknet, shutting down the second iteration of the underground black market Silk Road 2.0, and arresting its operator, a 26-year old former Google programmer. EC3’s challenge will be to continue making these high-profile arrests while adapting to the ever-changing array of techniques cybercriminals use.

SOURCES: : “FBI, Europol Make Large ‘Dark Web’ Bust,” Reuters, November 7, 2014; “Only 100 Cybercrime Brains Worldwide Says Europol Boss,” BBC News, October 10, 2014; “Service Model Driving Cyber Crime, Says Europol Report,” by Warwick Ashford, Computer-weekly.com, September 29, 2014; “Europol’s EC3 Launches Pan-Euro Cybercrime Taskforce J-CAT,” by Phil Muncaster, Info Security, September 2, 2014; “Europol Launches Taskforce to Fight World’s Top Cybercriminals,” by Tom Brewster, Theguardian.com, September 1, 2014; “First Year Report,” EC3, February 9, 2014; “Brian Honan Appointed Special Advisor to Europol Cybercrime Centre,” Net-security.org, October 10, 2013; “Europol Appoints McAfee’s Raj Samani as Cybercrime Advisor at EC3,” The Security Lion, October 8, 2013; “Spanish Police and Europol Arrest Cybercrime ‘Service Providers,’ Europol, September 27, 2013; “Europol-Interpol Cybercrime Conference Steps Up Policing in Cyberspace,” Europol, September 25, 2013; “European Cybercrime Center Targets Airline Ticket Fraud,” by Jeff Goldman, esecurityplanet.com, July 2, 2013; “International Network of On-Line Card Fraudsters Dismantled,” Europol, March 8, 2013; “European Cybercrime Centre Dismantles its First Criminal Network,” by Nerea Rial, neurope.eu, February 14, 2013; “Opening of the European Cybercrime Center – A Journey Begins,” by Neil Robinson, rand.org, January 11, 2013; “Europe’s Cybercrime Fighters Get New Digs... Complete with Faraday Room,” by John Leyden, theregister.co.uk, January 11, 2013; “Europe’s New Cybercrime Center to Open Its Doors This Week: EC3 To Act As Hub for EU-Wide Collaboration to Combat E-Crime,” by Natasha Lomas, TechCrunch, January 9, 2013.