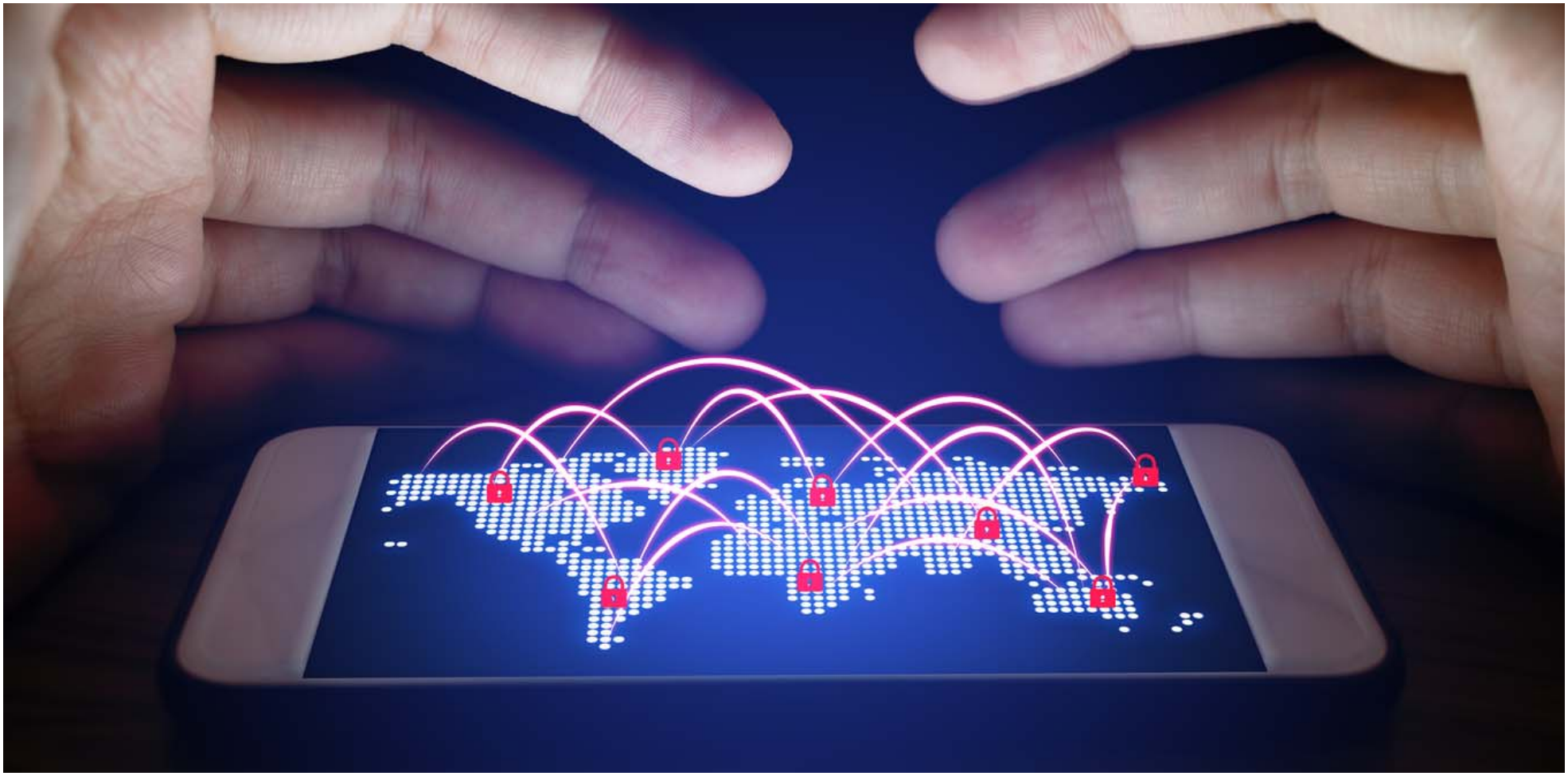
THE CONVERSATION
Academic rigor, journalistic flair



Police around the world learn to fight global-scale cybercrime

April 25, 2017 9.03pm EDT

Police must join forces across international borders to take on modern cybercriminals. wutzkohphoto/Shutterstock.com

From 2009 to 2016, a cybercrime network called Avalanche grew into one of the world's most sophisticated criminal syndicates. It resembled an international conglomerate, staffed by corporate executives, advertising salespeople and customer service representatives.

Its business, though, was not standard international trade. Avalanche provided a hacker's delight of a one-stop shop for all kinds of cybercrime to criminals without their own technical expertise but with the motivation and ingenuity to perpetrate a scam. At the height of its activity, the Avalanche group had hijacked hundreds of thousands of computer systems in homes and businesses around the world, using them to send more than a million criminally motivated emails per week.

Our study of Avalanche, and of the groundbreaking law enforcement effort that ultimately took it down in December 2016, gives us a look at how the cybercriminal underground will operate in the future, and how police around the world must cooperate to fight back.

Cybercrime at scale

Successful cybercriminal enterprises need strong and reliable technology, but what increasingly separates the big players from the smaller nuisances is business acumen. Underground markets, forums and message systems, often hosted on the deep web, have created a service-based economy of cybercrime.

Just as regular businesses can hire online services – buying Google products to handle their email, spreadsheets and document sharing, and hosting websites on Amazon with payments handled by PayPal – cybercriminals can do the same. Sometimes these criminals use legitimate service platforms like PayPal in addition to others specifically designed for illicit marketplaces.

And just as the legal cloud-computing giants aim to efficiently offer products of broad use to a wide customer base, criminal computing services do the same. They pursue technological capabilities that a

Authors

Frank J. Cilluffo
Director, Center for Cyber and Homeland Security, George Washington University

Alec Nadeau
Presidential Administrative Fellow, Center for Cyber and Homeland Security, George Washington University

Rob Wainwright
Director of Europol; Honorary Fellow, Strategy and Security Institute, University of Exeter

wide range of customers want to use more easily. Today, with an internet connection and some currency (bitcoin preferred), almost anyone can buy and sell narcotics online, purchase hacking services or rent botnets to cripple competitors and spread money-making malware.

The Avalanche network excelled at this, selling technically advanced products to its customers while using sophisticated techniques to evade detection and identification as the source by law enforcement. Avalanche offered, in business terms, “cybercrime as a service,” supporting a broad digital underground economy. By leaving to others the design and execution of innovative ways to use them, Avalanche and its criminal customers efficiently split the work of planning, executing and developing the technology for advanced cybercrime scams.

With Avalanche, renters – or the network’s operators themselves – could communicate with, and take control of, some or all of the hijacked computers to conduct a wide range of cyberattacks. The criminals could then, for example, knock websites offline for hours or longer. That in turn could let them extract ransom payments, disrupt online transactions to hurt a business’ bottom line or distract victims while accomplices employed stealthier methods to steal customer data or financial information. The Avalanche group also sold access to 20 unique types of malicious software. Criminal operations facilitated by Avalanche cost businesses, governments and individuals around the world hundreds of millions of dollars.

Low risk, high reward

To date, cybercrime has offered high profits – like the US$1 billion annual ransomware market – with low risk. Cybercriminals often use technical means to obscure their identities and locations, making it challenging for law enforcement to effectively pursue them.

That makes cybercrime very attractive to traditional criminals. With a lower technological bar, huge amounts of money, manpower and real-world connections have come flooding into the cybercrime ecosystem. For instance, in 2014, cybercriminals hacked into major financial firms to get information about specific companies’ stocks and to steal investors’ personal information. They first bought stock

in certain companies, then sent false email advertisements to specific investors, with the goal of artificially inflating those companies' stock prices. It worked: Stock prices went up, and the criminals sold their holdings, raking in profits they could use for their next scam.

In addition, the internet allows criminal operations to function across geographic boundaries and legal jurisdictions in ways that are simply impractical in the physical world. Criminals in the real world must be at a crime's actual site and may leave physical evidence behind – like fingerprints on a bank vault or records of traveling to and from the place the crime occurred. In cyberspace, a criminal in Belarus can hack into a vulnerable server in Hungary to remotely direct distributed operations against victims in South America without ever setting foot below the Equator.

A path forward

All these factors present significant challenges for police, who must also contend with limited budgets and manpower with which to conduct complex investigations, the technical challenges of following sophisticated hackers through the internet and the need to work with officials in other countries.

The multinational cooperation involved in successfully taking down the Avalanche network can be a model for future efforts in fighting digital crime. Coordinated by Europol, the European Union's police agency, the plan takes inspiration from the sharing economy.

Uber owns very few cars and Airbnb has no property; they help connect drivers and homeowners with customers who need transportation or lodging. Similarly, while Europol has no direct policing powers or unique intelligence, it can connect law enforcement agencies across the continent. This "uberization" of law enforcement was crucial to synchronizing the coordinated action that seized, blocked and redirected traffic for more than 800,000 domains across 30 countries.

Through those partnerships, various national police agencies were able to collect pieces of information from their own jurisdictions and send it, through Europol, to German authorities, who took the lead on the investigation. Analyzing all of that collected data revealed the identity of the

suspects and untangled its complex network of servers and software. The nonprofit Shadowserver Foundation and others assisted with the actual takedown of the server infrastructure, while anti-virus companies helped victims clean up their computers.

Using the network against the criminals

Police are increasingly learning – often from private sector experts – how to detect and stop criminals' online activities. Avalanche's complex technological setup lent itself to a technique called "sinkholing," in which malicious internet traffic is sent into the electronic equivalent of a bottomless pit. When a hijacked computer tried to contact its controller, the police-run sinkhole captured that message and prevented it from reaching the actual central controller. Without control, the infected computer couldn't do anything nefarious.

However, interrupting the technological systems isn't enough, unless police are able to stop the criminals too. Three times since 2010, police tried to take down the Kelihos botnet. But each time the person behind it escaped and was able to resume criminal activities using more resilient infrastructure. In early April, however, the FBI was able to arrest Peter Levashov, allegedly its longtime operator, while on a family vacation in Spain.

The effort to take down Avalanche also resulted in the arrests of five people who allegedly ran the organization. Their removal from action likely led to a temporary disruption in the broader global cybercrime environment. It forced the criminals who were Avalanche's customers to stop and regroup, and may offer police additional intelligence, depending on what investigators can convince the people arrested to reveal.

The Avalanche network was just the beginning of the challenges law enforcement will face when it comes to combating international cybercrime. To keep their enterprises alive, the criminals will share their experiences and learn from the past. Police agencies around the world must do the same to keep up.

Cloud computing **Cybersecurity** **Spam** **Police** **Cybercrime** **Ransomware** **US police** **DDoS** **Distributed Denial of Service (DDoS) Attack**