March 2017

Issue Brief # 2017 - 03

Responding to Cybercrime at Scale: Operation Avalanche – A Case Study

Robert Wainwright
Director
Europol

Frank J. Cilluffo
Director
Center for Cyber and Homeland Security

EUROPOL

Center for Cyber
& Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

Responding to Cybercrime at Scale:
Operation Avalanche – A Case Study

Robert Wainwright[1]
Director, Europol

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

Ransomware targeting individuals, businesses, and even hospitals. Large-scale cyber heists and malware attacks against banking systems and mobile devices. Internet of Things-powered botnets involved in launching some of the largest DDoS operations the internet has ever seen. Such headlines, in their countless iterations, plagued 2016. Looking back, one cannot help but wonder whether ever-shortening innovation cycles and the spread of technology into all aspects of daily life have enabled the significant growth in threats posed by cybercriminals.

The internet has connected societies and economies across the globe, profoundly changing the way humans communicate, interact and do business. Despite its many undeniably positive effects, the internet has helped to establish a reality of ubiquitous victimhood.[2] Near universal exposure makes everyone vulnerable to the growing threat posed by the intersection of traditional organized crime and the tools and expertise of modern cyber criminals. This pairing of threat and vulnerability has been exacerbated by the development of a service-based economy that facilitates low-risk, low-cost, and high-profit cybercriminality at a global scale.

Law enforcement has sought to combat this threat by promoting safety for online citizens, security for their digital assets, and justice for those who have been victimized. Strategies that focus on achieving these goals must include aspects geared towards prevention and deterrence, which in turn must be based on a thorough understanding of the motivations and operating procedures of cybercriminals. It is therefore important for law enforcement entities seeking to disrupt and deter malicious cyber actors to closely study the tactics, techniques, and procedures of cybercriminals through the lens of applicable business models. More critically, law enforcement must begin to conceptualize cybercrime as a true enterprise that cannot be neutralized simply by focusing on narrowly defined cases or interrupting transactions. Instead, these operations must be woven into broader strategies that leverage multi-pronged approaches capable of addressing the complex businesses criminal organizations resemble.

The recently concluded Operation Avalanche, in which an international coalition of law enforcement agencies and private sector partners neutralized one of the most sophisticated criminal syndicates in history, is a case worth studying. It is the most impressive in a recent string of cross-border, law enforcement led initiatives that has illustrated the importance of organizing responses to vast cybercrime networks based on the unique aspects of their business models. This issue brief will first provide background on the concept of Crime-as-a-Service (CaaS) and will then demonstrate how law enforcement used its understanding of this framework to successfully cripple the Avalanche platform. This brief concludes by drawing on lessons learned to present a path forward for coordinated efforts seeking to takedown cybercrime networks and deter cybercriminals in the first place.

[1] The authors would like to thank their respective staffs, who contributed to drafts of this report. This includes the staff of EC3 from Europol and Alec Nadeau, a Presidential Administrative Fellow at the Center for Cyber and Homeland Security. The authors would also like to recognize the support and insight provided by Flashpoint, which produced some of this report's figures.

[2] The widening of the pool of potential cybercrime victims as a result of the global proliferation of technology. *See* Mary Aiken, *The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behavior Changes Online*. Spiegel & Grau (2016).

Cybercrime from a Business Perspective – the Crime-as-a-Service Model

While achieving the benefits of cybercrime used to be relatively costly and was seemingly beyond the scope of traditional criminals, a market for illicit digital services has grown and matured, effectively leading to a profit-driven industrialization of cybercrime. As with legitimate economies, the cybercrime economy is driven by market forces and is capable of matching the needs of producers and consumers across the globe. The development of such an economy has allowed increasing numbers of criminals, including those with minimal technological savvy, to trade and utilize illicit digital services and tools.

The term Crime-as-a-Service is used to describe a service-based business model that supports the entire cybercrime value chain and drives the digital underground economy. It represents a dynamic and continuously evolving industry, characterized by a division of labor and specialization that produce a wide range of commercial and complementary services. The provision and monetization of such skills, tools, and expertise facilitates a broad range of cyber-enabled and cyber-facilitated crime – for example, hacking as a service, stolen credit card information, botnet rentals, etc. – as well as illicit online trade in drugs, weapons, stolen goods, counterfeit documents and child sexual abuse material.

Cybercriminal organizations have become increasingly complex and specialized as the financial rewards have dramatically expanded over the past decade. Previously, cybercriminals had to master multiple competencies in order to attack victims and extract profit from the cybercrime ecosystem. This created high barriers to entry for new cybercriminals and led to inefficient allocation of time and resources in the cybercrime economy.

Over time, cybercriminals came to understand that a division of labor would work well for their communities. First, actors can specialize in domains for which they have a comparative advantage or special talent, advancing the level of expertise in their particular area of specialization beyond what could be accomplished if each individual actor were responsible for all elements of the cybercrime chain. Second, the barrier of entry is lower for new participants because they can merely purchase the goods and services they need, as opposed to spending significant time and money building their own capacities. This environment is characterized by an increasing level of automation from the development of tools and services such as exploit kits and banking malware, to deployment services and monetization via money and packet mules or fences.

The CaaS model characterizes the operations of criminal online marketplaces, online fora, different types of communication channels, etc. which are complemented by anonymous payment mechanisms such as Bitcoin. The majority of these marketplaces are present in the Deep Web, a realm of the Internet that is un-indexed and inaccessible by common search engines, or the Darknet, a portion of the Deep Web that requires specialized software for access.[3] The criminal use of encryption and anonymization services and tools, including anonymity layer networks such as TOR, is a key characteristic of the model. These tools, many of which make up the backbone of the Deep Web and Darknet, allow criminals to mask their identity and location, hide their data, protect their communications and obfuscate their financial transactions, ultimately reducing their exposure to legal risks.

In general, there are two types of actors who support the infrastructure of marketplaces for cybercrime, the first being cyber criminals who provide technical know-how and experience in cyber-enabled operations. The second category captures traditional criminal organizations looking to leverage the digital underground economy to obtain the cyber tools and services necessary to expand their illicit business models into cyberspace. These organizations bring money, manpower, and networks to the table. Of course, these markets would not be able to function without the customer base of those

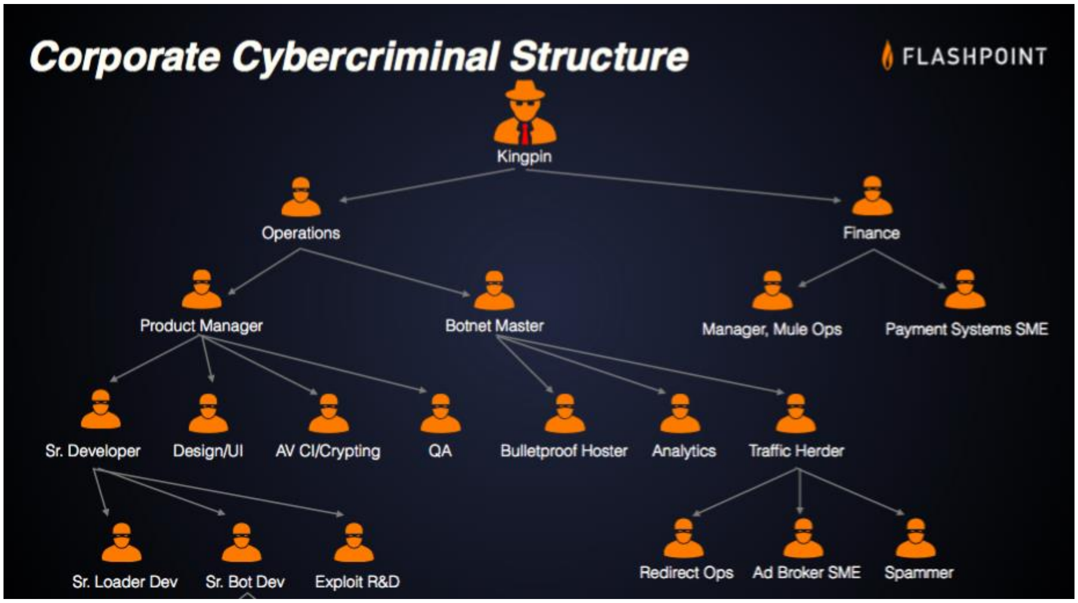
[3] "Illuminating the Deep and Dark Web: The Next Frontier in Comprehensive IT Security," *Flashpoint Intel* (2015), https://www.flashpoint-intel.com/book/illuminating-deep-dark-web.

seeking to purchase illicit materials, controlled substances, and criminal services. The CaaS model therefore offers profits and capacity to criminals of all types as well as non-criminal malicious actors.

The CaaS model has allowed cybercrime to develop into a sophisticated enterprise. Much like the Software-as-a-Service (SaaS) model, CaaS allows producers to achieve economies of scale which serves as yet another contributing factor to a shrinking barrier to entry for participants in the cybercrime market. This economic phenomenon has led CaaS to expand the breadth and depth of cybercrime's reach in modern society.

The entrepreneurial behavior of cybercriminals mimics legitimate business practices including customer service, online rating systems, advertisements and even special discounts.[4] Today, many cybercriminal syndicates are structured much like an IT company, with programmers, web designers, system administrators, and other roles found in legitimate enterprises. Indeed, many treat their cybercriminal activities as a career. Figure 1 is a representation of a cybercrime enterprise. At the top sits a kingpin, or CEO, in charge of all operations. This individual is a consummate businessperson who excels at maximizing profit, but often has very little understanding of the technical details involved in the business. The kingpin delegates work to an operations lead and a finance lead. Operations can be further divided into product development and botnet management, while the finance division controls fraud schemes and moves stolen money into the organization's accounts.

Figure 1: The Corporate Cybercriminal Structure



Moreover, there are indications that underground markets operate according to economic principles. For instance, the interaction of supply and demand serves as an efficient pricing mechanism for certain services, tools, and goods related to cybercrime. In the case of stolen credit card information, one can see these forces in action in the wake of large data breaches that drastically increase the supply of stolen financial information in underground markets. When the stolen credit card information of millions of victims is dumped into a market place, the shift in supply may lead to a new and lower overall equilibrium price, which will make it cheaper to buy certain categories of credit card information until supply levels normalize.[5] However, while there might be an overall price reduction due to market

[4] Roland Dela Paz, "Merry Cryptmas! CryptXXX Ransomware offers Christmas Discount," *Forcepoint Security Labs* (December 20, 2016), https://blogs.forcepoint.com/security-labs/merry-cryptmas-cryptxxx-ransomware-offers-christmas-discount.

[5] Jaikumar Vijayan, "The Identity Underground," *Passcode* (2015), http://passcode.csmonitor.com/identity-trade.

saturation, only minimum or no price fluctuation is to be expected in relation to premium cards, particularly if the information is very recent.

On the demand side of the equation, one must understand that criminals are looking for the cyber tool that maximizes their utility by providing them with the greatest potential to earn a profit. Therefore, one of the principal economic factors driving demand and determining demand elasticity of a cybercrime product is its return on investment relative to substitute goods or services. The surge in demand and popularity for ransomware is a good example of this factor. When cyber criminals began to demonstrate ransomware's potential to return significant profits relative to investments, demand for it grew rapidly.[6]

This entrepreneurial and relatively sophisticated marketplace has allowed traditional organized crime groups to step into cybercrime, without possessing the skill or capability to develop the necessary tradecraft in-house. It is now relatively cheap and convenient for these criminals to purchase the services and tools needed to support their criminal business, including training, franchise-type arrangements, ready markets and customized malware development.

Table *1* provides a simplified overview of how the various steps of the cybercrime value chain can be outsourced.

Table 1: Simplified Overview of the CaaS Model

Do it yourself	Malware as a Service	Botnet as a Service	Distribution as a Service	Crime as a Service
🟦 Collect and launder money	🟦 Collect and launder money	🟦 Collect and launder money	🟦 Collect and launder money	🟧 Collect and launder money
🟦 Distribute malware	🟦 Distribute malware	🟦 Distribute malware	🟧 Distribute malware	🟧 Distribute malware
🟦 Infect target machines	🟦 Infect target machines	🟧 Infect target machines	🟧 Infect target machines	🟧 Infect target machines
🟦 Develop and test malware	🟧 Develop and test malware	🟧 Develop and test malware	🟧 Develop and test malware	🟧 Develop and test malware

🟦 **Step managed by criminal**

🟧 **Step managed and provided as a service to criminal**

However, it is not just the technical aspects of cyberspace and existing business models that can facilitate criminality but also the way we behave online: cyber psychologists refer to it as the online disinhibition effect of cyberspace. This phenomenon makes criminals (and individuals in general) bolder, thanks to the perceived lack of authority online, the ease of assuming anonymity, and the sense of

[6] Maria Korolov, "Ransomware Took in 1 Billion in 2016- Improved Defenses may not be enough to Stem the Tide," *CIO* (January 5 2017), http://www.cio.com/article/3154988/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html.

physical distance from the actual crime scene and victims.[7] In combination with the low risk of detection, the potential for high profits, and a service-based underground economy that provides the necessary means, this has helped cybercrime to develop into an internationally thriving business, albeit an illegal one.

One way of describing progress is that it is either horizontal – doing more of the same that works - or vertical – doing new things or finding new ways to do something.[8] Unsurprisingly, the latter is harder to achieve and implies innovation, entrepreneurship, and adaptability. It is safe to say that cybercrime has successfully progressed vertically, certainly at a macro level. At a micro level, criminal entrepreneurship is often demonstrated by limited innovation using well-tested modi operandi that work. In fact it is often law enforcement that unintentionally acts as an incubator for innovation through successful operations against cybercriminals. The bottom line is that markets for cybercrime have matured around the Crime-as-a-Service model, allowing a wider variety of actors to engage in criminal activity that threatens a broader swath of the population.

Operation Avalanche – Takedown of an International Business Conglomerate

In December 2016, Europol and its main partners - the Public Prosecutor's Office Verden and the Lüneburg Police (Germany), the United States (U.S.) Attorney's Office for the Western District of Pennsylvania, the U.S. Department of Justice (DOJ), the U.S. Federal Bureau of Investigation (FBI), Eurojust and the Joint Cybercrime Action Taskforce (J-CAT)[9] – along with its network of international law enforcement and trusted private partners successfully executed one of the most technically complex takedowns in the history of cybercrime. The global operation targeted Avalanche – an international criminal business that had been active since 2009. This takedown required real-time coordination across more than 30 different jurisdictions and occurred on an unprecedented scale and scope. While Europol has demonstrated previous successes coordinating cross-sector, cross-border botnet takedowns, such as those against ZeroAccess (2013),[10] GameoverZeuS (2014),[11] and Ramnit (2015),[12] Operation Avalanche is in a different league for reasons discussed below.

Avalanche offered criminal infrastructure and services that its associates used to launch multiple cybercrime campaigns ranging from banking Trojans, to ransomware, phishing, and associated money laundering activities. The very essence of the Avalanche network and its CaaS operating model, with its varied portfolio of innovative products and services, pro-active advertising, and customer support features, is a striking example of how cybercriminal groups today work like international businesses.[13] Avalanche consists of more than 20 different firms, each representing one of the diverse malware

[7] John Suler. "The Online Disinhibition Effect." *Cyberpsychology & Behavior* 7.3 (2004). *See also* Mary Aiken, *The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behavior Changes Online*. Spiegel & Grau (2016).

[8] Blake Masters, and Peter Thiel. *Zero to One: Notes on Startups, or How to Build the Future*. Random House (2014).

[9] "Joint Cybercrime Action Taskforce (J-CAT): Fighting Cybercrime Around the World." Europol. https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce

[10] "Notorious Botnet Infecting 2 Million Computers Disrupted." Europol (December 5, 2013). https://www.europol.europa.eu/newsroom/news/notorious-botnet-infecting-2-million-computers-disrupted

[11] "International Action against 'Gameover Zeus' Botnet and 'Cryptolocker' Ransomware." Europol (June 2, 2014). https://www.europol.europa.eu/newsroom/news/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

[12] "Botnet Taken Down through International Law Enforcement Cooperation." Europol (February 25, 2015). https://www.europol.europa.eu/newsroom/news/botnet-taken-down-through-international-law-enforcement-cooperation; Luukas K. Ilves, Timothy J. Evans, Frank J. Cilluffo, and Alec A. Nadeau, "European Union and NATO Global CyberSecurity Challenges: A Way Forward," *PRISM Volume 6, No. 2* (July 28, 2016), http://cco.ndu.edu/News/Article/840755/european-union-and-nato-global-cybersecurity-challenges-a-way-forward.

[13] A conglomerate is a large corporation formed by a group of separate firms, often in different industries in order to diversify its business and to allow for economies of scale, while operating internationally and continuously modernizing and adapting its business model to ensure market domination and resilience

families the network was supporting,[14] and each providing core technical and financial services[15] to its globally dispersed customers on five continents.

Avalanche also employed a technically complex command and control infrastructure, which enhanced the criminal network's resilience to detection and takedown by the authorities. Its perceived, relative resilience in the face of law enforcement was a major part of Avalanche's competitive advantage, as it allowed the network to gain the trust of its customers. To date, this is the world's largest and most sophisticated cybercriminal syndicate law enforcement has encountered. It clearly underlines the growing audacity of cyber criminals, as well as their entrepreneurial character and ability to pioneer new techniques and monetize their skills.

As a case study, Operation Avalanche highlights how law enforcement authorities and their cybercrime divisions have also progressed vertically in their capacity to understand and neutralize a variety of technologically advanced criminal operations. As demonstrated by Europol and its dedicated European Cybercrime Centre (EC3), law enforcement is continuously developing cutting-edge approaches to respond to global cyber threats. The dismantling of the Avalanche cyber ring in particular marked the largest-ever use of what is called sinkholing,[16] a technique used to combat cybercriminal infrastructure by interrupting command and control channels. Operation Avalanche was unprecedented in its scale, with over 800,000 domains seized, sinkholed or blocked. Due to the size and worldwide dispersion of the network, the operation also temporarily disrupted the global cybercrime ecosystem.

In addition to its technical feats, what made this joint operation a distinct success for international policing was the identification and takedown of the alleged C-suite executive team of the network. This team included Avalanche's two Chief Executive Officers who administered the network, the Chief Operating Officer/Chief Technical Officer who provided key technical support to the administrators; and the two Chief Financial Officers, who oversaw the money mules and money laundering operations in general. By cutting off the head of Avalanche, law enforcement has prevented other members of the network from quickly re-establishing their criminal enterprise. This is a markedly better outcome compared to the typically speedy recovery and re-operationalization of criminal networks that often occurs when technical cybercriminal infrastructure takedowns are not accompanied by attribution and legal action. Law enforcement has learned that cybercriminal organizations tend to have business continuity plans that account for and minimize the impact of "business disruptions" caused by technical operations against criminal infrastructure. Therefore, in responding to Avalanche, law enforcement made sure that it was poised to not only disrupt command and control infrastructure, but also apprehend the network's C-suite, the effects of which business continuity plans cannot fully ameliorate.

Attribution of crime in cyberspace remains one of the core challenges facing law enforcement due to a wide range of legal, technical and internet governance issues. However, what can be called the "Uberization" of international policing[17] is allowing authorities, together with trusted third parties, to develop the advantages necessary to address the proliferation of cybercrime - and associated challenges such as attribution - by using the combined power of the network.

Europol and EC3 serve as an apt illustration of this networking concept. Similar to Uber which does not

[14] Most cybercriminal law enforcement actions focus on one particular malware family only

[15] Infrastructure with the capacity to launch a wide range of cybercriminal attacks and support for the laundering of the criminal proceeds

[16] Sinkholing is an action whereby traffic between infected computers and a criminal infrastructure is redirected to servers controlled by law enforcement authorities and/or an IT security company by assuming control of the domains used by the criminals. When successful, infected computers can no longer reach the criminal command and control computer systems. The sinkholing infrastructure captures victims' IP addresses, which can subsequently be used for notification and follow-up

[17] Robert Wainwright, "The 'Uberisation' of International Work," *Linkedin* (January 23, 2016), https://www.linkedin.com/pulse/uberisation-international-police-work-rob-wainwright.

own any vehicles or Airbnb which does not own any hotels, Europol has neither direct policing powers nor unique intelligence. Still, Europol has established itself as one of the leading law enforcement agencies worldwide, connecting more than 750 entities. Europol has been able to find success in the business of disrupting international cybercrime organizations because of its willingness to engage in cross-border partnerships that closely involve private sector representatives. Since its establishment in 2013, Europol's EC3 has adopted an inclusive intelligence-led response strategy. This strategy proved critical to the success of many international operations executed to date, including the Avalanche takedown.

While Europol serves as an illustration of the "uberization" concept as applied to international policing, Operation Avalanche shows how Europol can apply this concept to overcome the resilient business models of many cybercrime organizations. From its nascent stages, EC3 supported the international investigation and added particular value to its overall success by facilitating secure information exchanges among its many partners. It also coordinated operations and facilitated de-confliction of efforts. Moreover, EC3 served as the bridge between law enforcement entities and the relevant private partners participating in Operation Avalanche, bringing together authorities and expertise in a way that was instrumental to the takedown operation and subsequent victim remediation efforts. Bringing it all together, EC3 provided in-depth analysis and advanced digital forensic support, both of which were fundamental to mapping Avalanche's global criminal infrastructure and identifying key suspects.

Also of note, the actionable intelligence developed within the framework of the Avalanche investigation proved critical for US authorities to execute a major arrest against a high-value target suspected of using the complex GozNym malware. Dubbed at one point to be the superstar of the malware scene, the GozNym banking trojan is another example of an innovative "business" product. Authorities have recorded attacks against22 financial institutions in the US alone, based upon the GozNym malware. [18] The man behind GozNym was using the Avalanche malware distribution network, exemplifying the growing business acumen of cybercriminals. Because authorities properly secured electronic evidence, the US has successfully extradited the suspect, who is facing a sentence of up to 100 years in prison and a maximum fine of $3,500,000.[19]

In the context of the increasing influence of Crime-as-a-Service, the ultimate takeaway from Operation Avalanche is that law enforcement must work to understand the business models of cybercrime organizations if it is to undermine their activities. In this case, Europol and its partners responded to the distributed, specialized, and highly capable Avalanche network by leveraging a cross-border network of authorities and resources to target Avalanche's technical infrastructure and cybercriminal C-suite. The success of this operation represents progress in the realm of law enforcement's efforts to disrupt and deter international cybercrime, progress based on a keen understanding and appraisal of Avalanche's CaaS business model.

Conclusion

The success of Operation Avalanche, executed by EC3 together with its law enforcement and private partners worldwide, demonstrates how the axiom, "it takes a network to defeat a network," has never been more relevant. As new technologies are rapidly narrowing the gap between motivated offenders, suitable targets, and opportunities to commit cybercrime, international policing needs to employ innovative tactics in relation to apprehension, target hardening, and suppression in the context of

[18] Catalin Cimpanu, "GozNym Malware Faces up to 100 Years in Jail," Bleeping Computer (December 16, 2016), https://www.bleepingcomputer.com/news/security/goznym-malware-author-faces-up-to-100-years-in-jail/

[19] "Bulgarian Charged with GozNym Malware Attacks in the U.S.," Department of Justice, U.S. Attorney's Office Western District of Pennsylvania (December 12, 2016), https://www.justice.gov/usao-wdpa/pr/bulgarian-charged-goznym-malware-attacks-us.

cyberspace.[20] The growing sophistication of cybercriminal threats calls for a partnerships-based, multi-faceted and agile approach that goes beyond detection and disruption to encompass deterrence and prevention as well.

In doing so it is necessary to consider the business characteristics of cybercrime, particularly with respect to the emerging model of Crime-as-a-Service, to get a deeper understanding of the relevant trends and developments within the cybercriminal underground. This type of familiarity allowed law enforcement authorities to identify counter business strategies that they integrated into Operation Avalanche. Going forward, adaptable, cross-border partnerships that leverage this strategy will be more likely to mitigate the threats posed by increasingly entrepreneurial and sophisticated cyber criminals.

[20] Marcus Cohen and Lawrence Felson's Routine Activity Theory states that crimes are like to occur when a motivated offender, a suitable target, and absence of capable guardianship are present. The so called San Diego Wheel suggest three tactical avenues for addressing each of the three main elements – apprehension of offenders, making the suitable targets harder to reach, and suppression of the opportunities by regulating the environment or introducing new security measures

About the Center for Cyber & Homeland Security

The Center for Cyber & Homeland Security (CCHS) at the George Washington University is a nonpartisan "think and do" tank whose mission is to carry out policy-relevant research and analysis on homeland security, counterterrorism, and cybersecurity issues. By convening domestic and international policymakers and practitioners at all levels of government, the private and non-profit sectors, and academia, CCHS develops innovative strategies to address and confront current and future threats.

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu