FBI Cyber: Preventing Tomorrow's Threats Today

Categories : Articles

Date : September 19, 2016

Is the Federal Bureau of Investigation capable of defending the citizens of the United States of America against cyber-attacks? Are the cyber criminals of today too advanced and unpredictable for the FBI to keep up with? Is it possible for the FBI to predict and overcome such an advanced and ever-changing adversary? Although the cyber domain is challenging law enforcement in new and unpredictable ways, this paper imagines a future in which they are fully capable of combating cyber criminals. By reviewing past successes within the FBI, examining their ability to overcome jurisdictional hurdles, and analyzing their capacity to innovate and adapt to criminals who think they can outsmart them, the FBI of the future will be able to proactively prevent tomorrow's threats today.

Origins of the FBI

During the early 20th century, as the country began to widely adopt innovations such as automobiles and radios, which were science fiction just decades before, many American workers began moving into cities to capitalize on this increasing need to develop and maintain new technologies. The drastic influx of people into urban areas created cities with a multitude of citizens, packed into relatively small areas. As these cities began to grow, a new phenomenon began to develop as well: organized crime. Organized crime began to plague local authorities in unforeseen ways, and it became such an issue that the U.S. Attorney General was forced to intervene.[1]

The Bureau of Investigation, later renamed the Federal Bureau of Investigation (FBI), was the Attorney General's answer to organized crime. Founded in July 1908, the FBI was created to address the myriad of problems that local police authorities faced. In particular, the FBI dealt with criminals crossing state borders after committing a crime. During this period of early growth, the FBI primarily responded to crimes after they occurred without much thought to prevention and deterrence. One of the ways the FBI began to become more proactive was through the use of Identification Order No. 1, published in December of 1919.[2] What was essentially the FBI's first wanted poster provided an avenue for the organization to enlist public assistance and alert them to criminals, and this revolutionized the way the FBI would fight crime in the future. As the years progressed, the FBI quickly branched out and began to help local law enforcement authorities tackle different types of criminal activities. By the 1930's, the Great Depression's effect on the American economy began to heighten the problem of organized crime. The FBI began hiring experts from academia and industry on an as-needed basis to combat this growing threat and help them develop innovative crime fighting techniques. One example was Charles Appel who founded the FBI's first technical laboratory in 1932,[3] which gave them their first technical forensics

capabilities.

As the FBI began to build itself into a proactive crime fighting force, adaptability and innovation became the lynchpins of their core culture and effectiveness. Adaptability and innovation allowed the organization to become exceedingly proficient at its core competencies of robust investigations, and the ability to effectively interrogate suspects. Presently, a new wave of digital technologies is reshaping the very fabric of our world. Technologies like supercomputers and biometric scanners bring new dimensions to cyber. We now face threats in the cyber domain that were unimaginable during most of the twentieth century. The ability of the FBI to be proactive and continue with the adaptability and innovation it thrived on during its early years will determine the organization's success at adding the cyber domain to its list of core competencies.

The FBI Today

The innovation and adaptability integral to the early FBI helped to establish a new unit within their force capable of pursuing today's criminals operating in cyberspace. The FBI's Cyber Division was created in 2002, and has since refined their mission statement and improved the tools they possess. The Cyber Division pursues a three-part mission:

1. Coordinate, supervise, and facilitate the FBI's investigation of federal violations in which the Internet, computer systems, or networks exploited as the principal instruments or targets of terrorist organizations, foreign government-sponsored intelligence operations, or criminal activity, and for which the use of such systems is essential to that activity;
2. Form and maintain public/private alliances in conjunction with enhanced education and training to maximize counterterrorism, counterintelligence, and law enforcement cyber response capabilities;
3. Place the FBI at the forefront of cyber investigations through awareness and exploitation of emerging technology.[4]

By focusing on these guidelines, the FBI is becoming a formidable global cyber force. However, FBI Cyber continues to face obstacles. Even though new technologies make the world smaller, physical jurisdictional laws still apply. Furthermore, criminals are getting smarter, and their ability to leverage cyber is testing the limits of the FBI's capabilities.

In 2015, the Office of Personnel Management (OPM) was the victim of a data breach encompassing information from over 21 million federal employee records.[5] Speculation suggests the source of the attack originated in China, which posed challenges to the FBI due to their jurisdictional boundaries.[6] Because China is a sovereign entity, investigations cannot be carried out the same as if they were in the United States. Whether this was an intentional attack with the intent of metaphorically drawing cyber blood or just a show of force, the FBI must continue to follow international laws that dictate jurisdictional limits. That task is only made more difficult when the FBI cannot identify who is carrying out such attacks.

The OPM breach presented a new set of challenges as authorities struggled to identify the responsible party. The FBI is structured to deal with organized crime, but this provided a different scenario with the rise of powerful software that is accessible to nearly anyone. The list of possible suspects responsible for the OPM breach, and similar events, has exponentially expanded to include anyone with the time or resources from an unaffiliated hacking group, such as Anonymous, to even a foreign government entity. Accordingly, the FBI will have to change the way in which they pursue criminals because the threat could be as inconspicuous as a kid in his garage.

Unfortunately, the FBI currently acknowledges that they are heavily reactive in dealing with cyber-crimes.[7] They are overwhelmed by the number of cyberattacks occurring each day. The FBI does not have the ability to assign the necessary personnel to every case and instead must focus primarily on high impact cases.[8] Following the OPM breach, the FBI put a great deal of their energy into educating the Office of Personnel Management, and similar agencies, in the dangers of hackers, and how to protect themselves.[9] The problem with this plan of action is that the data has already been lost and is impossible to recover. A proactive strategy needs to be put in place so that individuals and organizations know how to protect themselves and their sensitive information beforehand. While this will not solve the bigger issue, it will likely slow down hackers. This is essential in a time when data and the security of personal data are of great concern.

However, sensitive data is not the only Achilles heel which the United States needs to protect. Today, almost everything is connected through the Internet. Amy Hess, the Executive Assistant Director of the Science and Technology Branch, addressed one of the concerns associated with today's interconnectivity: "With the widespread horizontal distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable individuals of all ages in the United States either to travel or to conduct a homeland attack."[10] Another concern of interconnectivity is health care records. Now that all health records are required to be electronic, if the proper protection is not in place then a great deal of personal information could be compromised. The FBI has explicitly stated that "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics."[11]

Today, FBI Cyber faces a myriad of challenges. From jurisdictional obstacles to dealing with an increasingly connected world, the FBI is challenged to use cyber capabilities to their utmost. Modern cyberspace is no longer a game of chess. There are millions of players, trillions of pieces to move, and the rules are unclear. However, the recently issued Presidential Policy Directive 41 names the FBI as the Federal lead agency regarding cases of significant cyber incidents. This will allow FBI Cyber to continue to move forward with innovation and adaptability leading the way into the 21st century.

The FBI of the Future

Looking forward, the future of the FBI's Cyber Division will be well-rounded and multifaceted. They will accomplish the mission of acting both offensively and defensively against criminals through

innovation and acting proactively against cyber criminals across the globe, while simultaneously combating the constant attacks on the United States national infrastructure.

The increasing number of devices connecting to the web, or the Internet of Things, is a very real phenomenon that is shaping technological infrastructure. From phones to watches, significant amounts of hardware are connecting to the Internet.[12] Consequently, the vast volume of data being transmitted and stored comprise the term Big Data. According to Kenneth Cukier, Big Data Editor for The Economist, “No area of human endeavor or industrial sector will be immune from the incredible shakeup that’s about to occur as big data plows through society, politics, and business. People shape their tools, and their tools shape them”.[13] As an integral aspect of modern culture, Big Data will be at the forefront of matters both economic and military, personal, and public. Looking towards the future, Big Data analytics will be crucial for FBI security operations, and other law enforcement agencies, digitally exposing and prosecuting cyber criminals with speed and accuracy. This stream of data will also be constantly targeted by cyber criminals both autonomous and organized. As more organizations move towards integrating digital systems, enormous amounts of information will be the ideal targets for criminals who are more resilient and resourceful than what the world has dealt with before. Long gone are the days where it was easy to pin the finger on the bad guy with little effort or investigative struggle.

The FBI of the future will respond with the utmost conviction in putting away criminals who manipulate technology to commit crimes. Just as they responded to the waves of organized crime that originated from the Prohibition Era, the FBI’s Cyber Division will mold itself to fit the missions at hand regarding cyber-criminal activities. Today, we have extremely coordinated crime syndicates of professional information thieves, and in the future the FBI will likely confront private corporations licensed to steal weapons development projects, or investigate secret foreign intelligence agencies, fighting a war over capturing retinal scan data of employees at classified facilities. Humanity is heading towards a society where the sole perpetrator of a cyberattack could be a somewhat uneducated, yet determined hacker, perhaps even a child. Furthermore, we could face criminals who brazenly break into internal systems, but then use IP addresses to disappear. The future will have criminals who work beyond not only physical jurisdictional boundaries but possibly even outside of interstellar boundaries. No matter what situation arises, FBI Cyber will adapt to these trends as they develop, and perhaps even before they develop.

The implementation of the FBI Cyber Division’s future technology will take full advantage of criminal patterns and the general public, much like the HAL supercomputer of Stanley Kubrick’s film *2001: A Space Odyssey*, with comfortable predictability and function control based on comprehensive Big Data analysis and algorithms executed seamlessly in real-time. Jurisdictionally, it is predicted that the needs for cybersecurity will awaken an evolution of critical infrastructure everywhere, where every important organization with data will establish its means to monitor cyber-crimes against itself. Soon enough, humanity may use palm scanners to enter our cars and homes. Universal facial recognition software distributed to law enforcement agencies could be an alternative to the classic form of identification that every citizen is required to carry. Borders

between nations and territories will feel seamlessly irrelevant given the reach of technology across the globe. As these developments occur and distributed to the FBI, it will be increasingly harder for a criminal to cover their tracks, giving the advantage to 'future' law enforcement. However, this degree of technological innovation can be a double-edged sword; it can improve and simplify life, or it can destroy lives with calculated, malicious use. The FBI will fervently expand their efforts nationally and abroad in its war against criminals behind the keyboard, subduing tomorrow's threats.

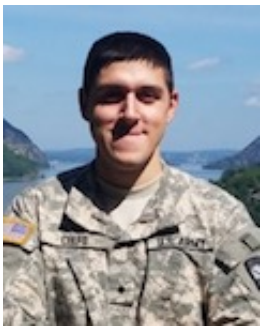
In the not so distant future, the nature of crime and punishment will change dramatically. With the continuing development of technological breakthroughs and society's rapid adoption of new ideas, we are moving closer towards making science fiction a reality. According to INTERPOL, "In the past, cyber-crime was committed mainly by individuals or small groups. Today, we are seeing highly complex cyber-criminal networks bring together individuals from across the globe in real-time to commit crimes on an unprecedented scale".[14] Ideally, the FBI will have its own team of highly skilled hackers who can infiltrate the confines of the Dark Web and proactively foil what attacks would occur. Perhaps the FBI will infiltrate the world of the Dark Web as an undercover user much like they did with the Italian mob in New York with the sting operation as depicted in the film *Donnie Brasco*, named after the undercover officer's criminal alias. The calculated combination of offensive operations on the Dark Web and the reinforcement of critical information systems and technology around the globe is the hallmark of a solution to a constantly evolving problem. Once cyber is infused into all aspects of the FBI, such as investigations, forensics, call centers, dispatching, and analysis fusion centers, the FBI Cyber of the future will then be recast into pursuing the next generation of criminals who attempt to thwart the FBI with even newer more clever ways. So criminals beware…

Acknowledgment

The authors would like to thank Richard Jacobs, Assistant Special Agent in Charge of the FBI Cyber Branch, for his support and encouragement throughout the writing of this paper. Richard Jacobs and his team of dedicated cyber agents provided us with the inspiration for this paper. And even though this paper focuses entirely on the FBI's foray into cyberspace, we believe the conclusions of this paper apply justly to any organization currently delving into cyber domain.

About the authors

Cadet Zoe Schorr is a summer intern at the Army Cyber Institute. She studies Traditional Mathematics at Worcester State University. Her research interests include robotics and World War II cryptography.



Nicholas Celfo is a Second Classman at the Virginia Military Institute in Lexington, VA. Majoring in Computer Science and seeking a minor in Computer Engineering, Cadet Celfo is beginning his 3rd year of collegiate study and Army ROTC in August 2016. Upon commissioning from VMI, he has a deep desire to branch into Army Cyber. A dedicated member of the VMI Regimental Band as a tuba player and the VMI Regimental Color Guard as a Sergeant, Nick traveled to Pasadena, California with the VMI Band to march in the annual Tournament of the Roses parade in January 2016. He feels extremely grateful to have interned at the Army Cyber Institute (ACI) at West Point in the summer of 2016 and welcomes any opportunity to return to the ACI or West Point in the future with open arms.

Conrad Kress is an Army ROTC Cadet studying at the University of Alaska, Anchorage. He is pursuing a Bachelor of Science in Mathematics, with research interests in the area of mathematical physics and quantum information science. As a cadet, Conrad has had the opportunity to attend the U.S. Army Airborne School, the Cadet Leader Course, and the ROTC Cyber Internship Program at the Army Cyber Institute. He has also served in cadet leadership positions including Platoon leader, Operations officer, Executive officer and Battalion Commander.

Cadet Keenan Wresch is working as an intern with the Army Cyber Institute. He attends Purdue University studying Computer Science and Physics. His research interests include cryptology and operating systems.

Lieutenant Colonel Ernest Y. Wong is the Chief of Staff at the Army Cyber Institute and an Assistant Professor with the Department of Systems Engineering at the United States Military Academy. He holds a B.S. in Economics from USMA, a M.S. in Management Science & Engineering from Stanford, a M.A. in Education from Stanford, and a Master of Military Science from the Mubarak Al-Abdullah Joint Command & Staff College in Kuwait. He had the opportunity to work as a NASA Summer Faculty Fellow and has served as a Military Intelligence Officer in the U.S. Army with overseas deployments to Iraq, Kuwait, and the Republic of Korea.

References

[1] Online Highways LLC. n.d. FBI. http://www.u-s-history.com/pages/h3866.html (accessed July 28, 2016).

[2] Federal Bureau of Investigation History. n.d. The FBI and the American Gangster. https://www.fbi.gov/history/brief-history/the-fbi-and-the-american-gangster (accessed August 15, 2016).

[3] Ibid.

[4] Jana D. Monroe, 2003. "The FBI's Cyber Division." FBI Archives. July 17. https://archives.fbi.gov/archives/news/testimony/the-fbis-cyber-division (accessed July 26, 2016).

[5] Sean Lyngass, 2016. "What DHS and the FBI learned from the OPM breach." The Business of Federal Technology. January 11. https://fcw.com/articles/2016/01/11/dss-opm-hack-lessons.aspx (accessed July 25, 2016).

[6] Federal Bureau of Investigation Cyber Division. n.d. "Ransomware." IC3. https://pdf.ic3.gov/Ransomware_Trifold_e-version.pdf (accessed July 27, 2016).

[7] Richard Jacobs, FBI Assistant Special Agent in Charge, Cyber Branch, office call and discussions with author, July 14, 2016.

[8] Sean Lyngass, 2016. "What DHS and the FBI learned from the OPM breach." The Business of Federal Technology. January 11. https://fcw.com/articles/2016/01/11/dss-opm-hack-lessons.aspx (accessed July 25, 2016).

[9] James Twist, Matthew Hutchison, Blake Rhoades, and Ryan Gagnon. 2016. "Why Government Organizations Don't Care: Perverse Incentives and an Analysis of the OPM Hack." The Heinz Journal 84-109.

[10] Amy Hess, 2016. "Deciphering the Debate Over Encryption." FBI. April 19. https://www.fbi.gov/news/testimony/deciphering-the-debate-over-encryption (accessed July 26, 2016).

[11] Federal Bureau of Investigation Cyber Division, 2014. "Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain." AHA. April 8. http://www.aha.org/content/14/140408--fbipin-healthsyscyberintrud.pdf (accessed July 28, 2016).

[12] Jacob Morgan, 2014. "A Simple Explanation of 'The Internet of Things'." Forbes. May 13. http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#3f919bd56828 (accessed July 26, 2016).

[13] Kenneth Cukier, 2015. "Big Data and the Future of Business." Technology Review. June 30.. https://www.technologyreview.com/s/538916/big-data-and-the-future-of-business/ (accessed July 26, 2016).

[14] Interpol. n.d. "Cybercrime." Interpol. http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (accessed July 26, 2016).