An Executive Cyber Education Framework for the Federal Bureau of Investigation

Mathias M. Boehm

Executive Summary

The Federal Bureau of Investigation (FBI) is crucial part of the nation's effort to protect national interests against malicious cyber actors. The challenge faced by the FBI is immense and for it to be successful its leaders must adopt a dynamic approach to education and collaboration with private industry. The cyber environment is very fluid, and adversaries are abundant. The FBI's Cyber Division has emerged as the primary investigative agency for cyber-crime and cyber-facilitated crime and while training and education are robust and continuously evolving, some shortcomings have a constraining effect on the FBI's security posture. To better prepare FBI leadership for contending with adversaries in the coming decades, education must emphasize a multilateral approach to cybersecurity and incorporate private industry as much as possible.

Problem Statement

The FBI is on the forefront of the nation's efforts to thwart cybersecurity threats both foreign and domestic. The cyber security domain represents a uniquely challenging landscape as the capabilities of adversaries are constantly increasing while our own mitigation measures can be slow to keep pace. The problem is simply enormous, and in order for the FBI to be effective in combating these vast threats, its leadership must receive the education and tools they need to react and implement effective policies and guidance. What kind of executive education must take place for the senior leaders of the FBI to implement an agile and proactive approach to cyber security? Also, how will FBI senior leaders adopt a holistic whole-of-society approach to address problems that are far too broad and deep for the US Government to address unilaterally?

The aim of this paper is to identify any inadequacies in cybersecurity training, specifically regarding the training of executive leadership. To accomplish this, this paper will describe the FBI's cyber security landscape and the current approach to cyber training. Through research and a series of

interviews, I intend to identify what measures need to be taken to address the shortcomings in executive training.

Approach Pursued

Most of the work behind this Critical Challenge Project consisted of open source research, interviews, polls, and a reflection of my own experiences. Open source research was the biggest component of this study with most of the information found on public Department of Justice and FBI sites. Information about the environment, current state of affairs and the adversaries the FBI cyber workforce contends with was drawn from public sites as well.

Interviews with FBI executive management was another crucial component of this study. As this CCP aims to address the existing shortcomings in executive education, gaining an understanding of the current educational framework from executives that have experienced it themselves is a necessary step in identifying ways it needs to be improved. I have endeavored to interview an FBI employee at every tier of the workforce including Special Agents working cyber cases, Supervisory Special Agents, Assistant Special Agents in Charge as well as Unit Chiefs overseeing executive and cyber education users.

I have conducted approximately polls with approximately 12 FBI employees that either work in cybersecurity or have demonstrated an interest in pursuing an advanced degree in cybersecurity. To gauge the interest in EMCS and to identify the factors that discourage employees from applying, I have asked each participant a series of questions which are outlined in the conclusion portion of this paper.

Finally, I've drawn heavily from my own experiences. I have reflected on my initial training at the FBI Academy, the various Information Security and Insider Threat awareness classes I've had to take to meet annual security training and my general perception of the current state of the cybersecurity landscape. My observations of the current disposition of the industry are based on my extensive public outreach that I routinely conduct with private companies in my area of responsibility.

Since information about the FBI and its practices is often classified, I have had to work under strict dissemination constraints. Despite various attempts, I did not obtain authorization to disclose some pertinent initiatives and partnerships the FBI is pursuing to improve executive education. One of my recommendations offered to promote a broader approach to executive education is a collaboration between the FBI and Brown University's EMCS program, though I have concluded that propositions such

as these require a process that takes several years. Consequently, I was unable to deliver what I was hoping would be an enduring collaboration. Though members of executive management have largely been forthcoming and very supportive of my CCP, all those I have interviewed have declined to be formal advisors.

The Current Cyber Environment

The Domain and FBI Priorities:

As the lead federal agency for investigating cyber matters, the FBI has developed a set of priorities to focus its efforts on. The current key priorities are Computer and Network Intrusions and Ransomware.

The FBI estimates that billions of dollars are lost as a result of network intrusions. These intrusions are the prototypical cyber violation and they can have a criminal, espionage or terrorism nexus. The threat actors in these cases are just as varied and can range from a single individual keen on obtaining notoriety among hackers to dedicated military units whose sole purpose is to gain access into their adversaries' systems.

The Department of Justice published a press release for a case in which two Chinese hackers with the Ministry of State Security (MSS) were charged with conducting computer intrusion operations that targeted intellectual property and confidential business information[1]. The incident from which the charges stemmed is a component of a prolonged technology theft campaign. The defendants Zhu Hua and Zhang Shilong are alleged to be members of the Advanced Persistent Threat 10 hacking group, also known as APT 10. The press release outlines their activities as follows:

"Over the course of the Technology Theft Campaign, which began in or about 2006, Zhu, Zhang, and their coconspirators in the APT10 Group successfully obtained unauthorized access to the computers of more than 45 technology companies and U.S. Government agencies based in at least 12 states, including Arizona, California, Connecticut, Florida, Maryland, New York, Ohio, Pennsylvania, Texas, Utah, Virginia and Wisconsin. The APT10 Group stole hundreds of gigabytes of sensitive data and information from the victims' computer systems, including from at least the following victims: seven companies involved in aviation, space and/or satellite technology; three companies involved in communications technology; three companies involved in manufacturing advanced electronic systems

and/or laboratory analytical instruments; a company involved in maritime technology; a company involved in oil and gas drilling, production, and processing; and the NASA Goddard Space Center and Jet Propulsion Laboratory."[2]

Ransomware has become rampant and is the FBI's second key priority. Ransomware is a form of malware that after being introduced to a system or network prevents their normal use. Attackers will usually demand money before relinquishing control of the network to the legitimate user. Ransomware can be introduced through a number of ways, most typically via a multi-lateral social engineering or phishing attack. Emails were once the most common vector for ransomware delivery, but the advent of more sophisticated spam detection programs has forced hackers to adapt and introduce the malicious code through other means.

Regardless of how ransomware is delivered, it will make a system inoperable until payment is received by the attackers. Any system can fall prey to a ransomware attack and victims range from small businesses to governments. One of the most significant ransomware attacks in recent memory is the 2018 ransomware incident in Atlanta, Georgia. Following infection, several key city systems were disabled. Affected systems included online bill payment, internet access and hazard reporting sites, through the attackers did not disable any emergency services[3]. Another example of a well-known ransomware attack is the WannaCry worm. This attack affected over 230,000 computers in more than 150 countries and has been attributed to the Democratic People's Republic of Korea (DPRK)[4].

Besides combating network intrusions and malware, the FBI Cyber Division is involved in a wide array of other law enforcement and national security efforts. It is not uncommon for terrorism, public corruption, and organized crime cases to have a strong cyber influence. Violent Crimes Against Children (VCAC) is an example of a type of criminal investigation that almost always involves cyber, even though those cases are traditionally run by agents in the Criminal Division. Even in Special Agents in the Cyber Division do not manage one of the aforementioned cases, they will often serve in an advisory capacity to the case managers.

Many Counter Intelligence (CI) cases are predicated by information obtain from a case owned by the Cyber Division. Espionage has become increasingly technical and it is often difficult to determine whether a Counter Intelligence case that involves Cyber is better managed by CI or Cyber. CI and cyber will often work jointly on cases in which there is not a clear preference to one or the other.

Cyber cases are further separated into criminal and national security categories. Criminal cases contend with criminals trying to make financial gain through cyber means whereas national security cases involve state-sponsored hackers

Adversaries

China: Perhaps the most infamous hacking unit to have made the news recently is Unit 61398, 3rd Department of the People's Liberation Army (PLA) of the PRC[5]. This unit gained international attention in 2014 when the US Department of Justice filed criminal charges against known state actors for the first time. As the primary agency for cyber matters, the FBI conducted the investigation.

The indictment of the five Chinese hackers alleges that "the defendants conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs). In some cases, it alleges, the conspirators stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen. In other cases, it alleges, the conspirators also stole sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity"[6]. The hackers were indicted for violations of several statutes, most notably 18 U.S.C. § 1030(B), Conspiring to commit computer fraud and abuse; 18 U.S.C. § 1030(a)(2)(C), Accessing a protected computer without authorization to obtain information for the purpose of commercial advantage and private financial gain; and 18 U.S.C. § 1030(a)(5)(A), Transmitting a program, information, code, or command with the intent to cause damage to protected computers.

Despite China having denied the existence of PLA hacking units, this case and a report from the cybersecurity firm Mandiant released in 2013, have exposed Unit 61398 and its operations to the world[7]. China is not the only state actor engaged in network intrusions. Russian hackers have been conducting intrusion attacks on the US electric grid, water processing plants, air transit and other components of our critical infrastructure[8].

Russia: Russia may not have great confidence in the outcome of a potential military confrontation with the US, but it has amassed considerable asymmetric power in cyberspace. Their hacking capabilities are made more frightening because their apparent intent to develop the ability to inflict grave harm to our critical infrastructure.

According to an article published by the Wall Street Journal, the US Department of Homeland Security (DHS) asses that hackers working for Russia infiltrated the control rooms of electric utility companies[9]. Not only did these hackers manage to reach key utility systems, they were able to elevate their permissions to the point where they were effectively in control. Had they wanted to, they could have easily "thrown the switch" and disrupted power flows[10].

Attacks such as the one described above are already very disruptive and cause grave economic harm to industry. It is likely that Russian hacking operations are a concerted effort to set conditions for a possible future confrontation. In effect, by insinuating themselves deeply into our systems the Russians are conducting something the military calls Operational Preparation of the Environment (OPE). OPE is defined as "nonintelligence activities conducted to plan and prepare for potential follow-on military operations"[11].

FBI Cyber Enforcement Challenges: Going Dark

Law enforcement has long relied on legal authorities to conduct investigations. One of the landmark amendments to the US constitutions which has really defined how law enforcement is permitted to conduct its investigations is the 4th Amendment which guarantees: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probably cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"[12]

One tool available to law enforcement investigators is the "wiretap" as authorized by Title III of the Omnibus Crime Control and Safe Streets Act of 1968[13]. This act establishes procedures for obtaining warrants to authorize wiretapping by governmental agencies and regulates the disclosure and use of authorized intercepted communications. In essence, the interception of wireless or telephonic communications is regulated by this act and it is designed to ensure that procedures are followed so as not to infringe on the right against unreasonable search and seizure under the 4th amendment.

Many cases relay on the interception of communication of investigative subjects. Traditional wiretaps are only practical when intercepting communications of telecommunications carriers, providers of interconnected voice over internet protocol (VoIP) and broadband access services[14]. Messaging platforms with end to end encryption do not afford law enforcement the same access to

communications are the aforementioned services do due to technical constraints and challenges to the limitations of existing laws that govern the interception of communications.

This has become a significant challenge for law enforcement and has been characterized as "Going Dark". Going Dark has rendered the legal interception and access to communications pursuant to a court order ineffective because law enforcement often lacks the technical ability to carry out and execute court orders because of constantly advancing communications services and technologies[15].

Going Dark applies to real-time data interception as well as stored communications. While the FBI is not keen on undermining the privacy of communications, Going Dark has also drastically diminished ability to "quickly obtain valuable information that may be used to identity and save victims, reveal evidence to convict perpetrators, or exonerate the innocent"[16]. The question of whether the US Government can compel a company to create the means for law enforcement to access an otherwise inaccessible device came to capture national attention in the wake of the San Bernardino shootings in December 2015[17].

Going Dark is certainly not the FBI's only cyber enforcement challenge. The agency must also contend with crimes that a largely cyber-facilitated such as VCAC, more commonly termed as child pornography. Even passive consumption of pornographic images of children is classified as a violent crime by the DOJ. The third cyber enforcement challenge is the rise of computer facilitated identity theft.

Disposition of the FBI

The FBI: The Federal Bureau of Investigation is the domestic intelligence and security service of the United States. While the FBI's origins lie in traditional law enforcement efforts such as combatting organized crime and investigating bank robberies, the agency has evolved and expanded across a wide domain. In addition to being the principal law enforcement agency, the FBI is also a member of the Intelligence Community (IC) and reports to both the Attorney General (AG) and the Director of National Intelligence (DCI), who overseas and coordinates all intelligence efforts of the IC. The FBI has primacy over national counter-terrorism (CT), counter-intelligence (CI) and Cyber efforts.

Each of the 56 field offices is under the command of the Special Agent in Charge (SAC). The SAC is responsible for overseeing all FBI activity in his or her office's Area of Responsibility (AOR). In addition to overseeing all investigative matters, the SAC must also establish and maintain relationships with the

community and its leaders, other law enforcement agencies and the various other partnerships the FBI relies on. The only FBI field offices that do not follow this organizational structure are the three largest, Washington DC, New York and Los Angeles. These are overseen by an Assistant Director in Charge (ADIC) is supported by SACs and their subordinate ASACs.

SAC's are considered senior leaders in the FBI and are the first level of employee classified as Senior Executive Service (SES). Many other SES positions besides SAC exist within the FBI and each of these positions is considered a key leadership or management position. The United States Office of Personnel Management (OPM) states the purpose of the SES is to "ensure that the executive management of the Government of the United States is responsive to the needs, policies, and goals of the Nation and otherwise is of the highest quality"[18].

SES's essentially oversee the federal government and serve as a crucial link between Presidential appointees and the general workforce. The SES is they key audience that will have to be convinced to affect significant change in cyber security and other policies.

The FBI is comprised of several branches, each overseeing several divisions or groups that are largely aligned along the same lines of effort. The National Security Branch's (NSB) mission is to "Detect, deter, and disrupt national security threats to the United States and its interests"[19]. The two main investigative units in the NSB are the Counterintelligence and Terrorism divisions. As the name implies, the Counterintelligence Division is tasked with understanding and mitigating threats posed by foreign intelligence services and their proxies. The Terrorism Division's responsibility is to dismantle domestic and international terrorist networks and cells. Combating terrorism became the FBI's top investigative priority after the September 11 attacks and it has remained the priority ever since. However, as cyber threats evolve and become more and more pervasive, the national strategy may pivot and realign investigative priorities.

The Criminal, Cyber, Response and Services Branch is comprised of the Criminal Investigative Division (CID) and the Cyber Division (Cyber) and other service related units. CID and Cyber are the operational investigative units within this branch while the others are charged with the management of specific support functions. As criminals and foreign state actors increasingly use a diverse array of sophisticated techniques to achieve their objectives, the traditional distinction between national security, criminal and cyber matters is becoming more and more blurred. The Cyber Division has

garnered the increased attention of policy and law makers as cyber matters are brought to the forefront of national awareness.

Cyber Division: Given the large number of federal law enforcement entities, it is important that primacy over a particular violation is assigned to a particular agency. In some cases, several agencies may have oversight over a violation. The salient example for this are drug cases which are investigated by both the FBI and the Drug Enforcement Administration (DEA). Even in those instances, one agency will typically be the lead for that violation even though other agencies may also work it.

The President's National Strategy to Secure Cyberspace is a publication released on February 14, 2003 that suggests ways that entities across the US can secure computer systems and networks. In addition to promoting public cyber security education, it established the role of law enforcement agencies in the cyber security domain. The strategy states that "The Department of Justice and the FBI lead the national effort to investigate and prosecute cybercrime"[20].

The FBI's Cyber Division was created in 2002 and has gone through drastic changes since its inception. A significant challenge for any component of the government, in particular for law enforcement, is keeping pace with emerging techniques, tactics and procedures.

The FBI's official site outlines role of the Cyber Division as follows: "The FBI is the lead federal agency for investigating cyber-attacks by criminals, overseas adversaries, and terrorists. The threat is incredibly serious—and growing. Cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated. Our nation's critical infrastructure, including both private and public sector networks, are targeted by adversaries. American companies are targeted for trade secrets and other sensitive corporate data, and universities for their cutting-edge research and development. Citizens are targeted by fraudsters and identity thieves, and children are targeted by online predators. Just as the FBI transformed itself to better address the terrorist threat after the 9/11 attacks, it is undertaking a similar transformation to address the pervasive and evolving cyber threat. This means enhancing the Cyber Division's investigative capacity to sharpen its focus on intrusions into government and private computer networks."[21]

Another way in which the FBI established itself as the lead investigator of cybercrime was by the establishment of the National Cyber Investigative Joint Task Force (NCIJTF)[22]. Officially established in 2008, the NCIJTF is comprised of over 20 agencies from across the IC, Department of Defense (DOD) and

Law Enforcement (LE). The task force has the responsibility to "to coordinate, integrate, and share information to support cyber threat investigations, supply and support intelligence analysis for community decision-makers, and provide value to other ongoing efforts in the fight against the cyber threat to the nation."[23] The NCIJTF is instrumental in pursuing those that seek to exploit the cyber domain to achieve criminal objectives, conduct espionage or carry out terrorist attacks. The NCIJTF leverages strong relationships with its international partners and the private sector to bring all available resources to bear against international and domestic cyber threats.

Cyber Training: Cyber awareness training is an integral part of the mandatory professional education that every employee of the FBI must complete annually. The past few iterations of cyber awareness training have always been delivered in the form of an interactive presentation that an employee can take at their discretion, the only requirement being that the training is completed by the posted deadline. In order to receive credit for the class, an employee must take a test and answer at least 80% of the questions correctly. The target audience of this training is the entirety of the FBI and not specific to those working cyber matters. The content of the training is not unlike that which many private corporations present to their employees. Employees are taught about common attacks like phishing, social engineering and elicitation techniques. Insider threat awareness is another facet of security training. As an intelligence agency, FBI employees present lucrative targets for foreign intelligence services. As such, every employee is taught how to recognize when they are being targeted for recruitment and to recognize people that exhibit vulnerabilities to or indications of compromise.

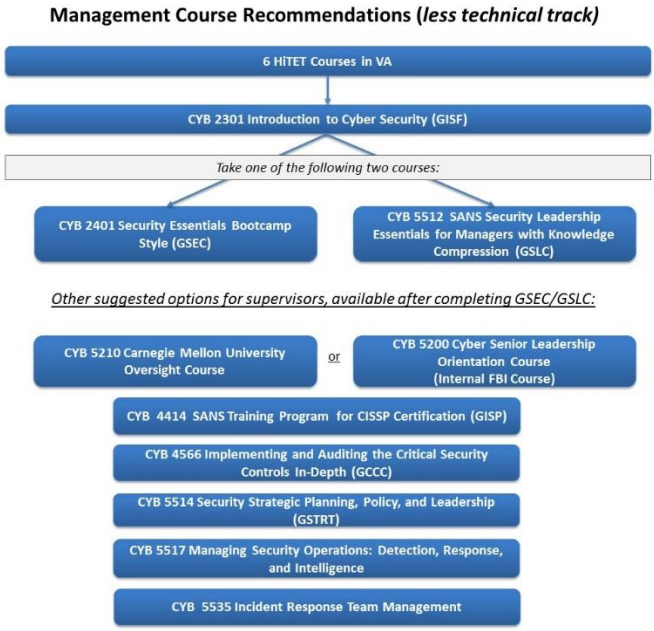
During their initial training at the FBI Academy in Quantico, Virginia, all agent trainees receive some rudimentary cyber security training to prepare them for duty in the field. While most new Agents find themselves assigned to squads that investigate criminal cases, some are sent directly to cyber squads. No certification is required for an assignment to work cyber matters, but Agents with a background in Science, Technology, Engineering and Math (STEM) are preferred.

The training received at Quantico hardly suffices to equip a cyber agent with the tools and knowledge to be effective. There are considerable training opportunities available to employees as they began their careers working cyber matters. An initial cyber assessment is administered to each new cyber agent and analyst and the level of training received depends on the employee's proficiency.

Cyber training is managed by the Cyber Education and Training Unit (CETU). This unit has collaborated with the SANS Institute[24] (SANS) to provide a wide range of technical courses to the FBI.

The goal of the partnership is to enhance the cyber and information security knowledge base of the FBI's cyber workforce. The Cyber SANS training program is available to members of the Cyber Division, Special Agents and Supervisory Special Agents working cyber intrusion cases full time in the field, computer scientists embedded in cyber squads and FBI Executive Management who oversee cyber operations.

Management Training: CETU has designed a training track specifically tailored to cyber managers. These courses do not delve as deeply into the technical aspects of cyber security as those meant for Special Agents and Intelligence Analysts. The program focuses on the skills needed to manage cyber investigators and to develop comprehensive cyber security strategies. The following chart captures the management course recommendations outlined by CETU:



The majority of the management courses is comprised of SANS courses. The six courses referred to as HiTET are taught online via Virtual Academy, the FBI's proprietary platform for online courses. Virtual Academy offers a wide array of courses for professional development. Mandated Insider Threat and Information Security (INFOSEC) courses are also delivered via Virtual Academy.

Managers are expected to know enough about their domain to be able to evaluate the progress of cases and offer effective guidance to their subordinates. They must become familiar with the tools

and resources available to aid case agents in their investigations and be able to recommend a course of action if the agent comes across a challenging issue that he or she needs help with. A manager must also be familiar with the FBI policies that all agents must adhere to.

Executive Education: The FBI has recognized the need for professional development across all tiers of leadership. This includes leaders at the executive and SES level who regularly participate in leadership symposiums in which new trends and challenges are discussed. The annual SAC's conference is an example of such a symposium which gives every SAC the opportunity to highlight issues of growing concern in their respective areas of responsibility. The conference also features guest speakers and subject matter experts that discuss topics that are likely to affect the agency in its entirety. Cybersecurity topics are a regular feature of SAC conferences as cyber is becoming an inextricable aspect of nearly all violations the FBI investigates.

Executive education is also bolstered by the FBI's Executive Programs Instruction Unit (EPIU). The EPIU's mission is to provide ongoing instruction to executive management by sponsoring training events and continuing education. The EPIU does not develop courses that are specifically tailored for cyber security issues.

Findings

Education and Training shortcomings

My research indicates that training and education initiatives to prepare the FBI workforce to be successful in the cyber domain are trending positively. Recent high-profile indictments of Chinese hackers and Chinese telecommunications conglomerate Huawei portend the US's intent to do more to mitigate the threat posed by China's technology theft campaign. FBI senior leadership has recognized the need to prioritize cybersecurity threats and this posture has become apparent in executive education, as shown by the increase of cyber topics presented during executive education.

Another indicator of cybersecurity progress is the FBI's Cyber On the Job Training (OJT) program. The OJT's objective is to permeate cyber security capability beyond the confines of the Cyber Division. If an employee elects to participate in Cyber OJT, he or she will spend a year in cyber training which consists of a "Cyber Boot Camp" and several SANS courses. Upon completing the program, the employee will receive a comprehensive education in cybersecurity with a few basic certifications.

Despite the positive trends, I have identified some training shortcomings that if rectified would increase the cybersecurity awareness level of the entire FBI workforce. Infosec and Insider Threat

training courses are delivered via a self-paced course and must be successfully completed on an annual basis. The classes only change every few years and the subsequent tests can be retaken several times which means that there is nothing from precluding an employee from skipping the curriculum and going directly to the test and taking it as many times as needed to pass. If an employee does not complete the training, he or she does not lose access to their accounts and case management systems.

Executive education provided to FBI's leaders underscores the need for collaboration with private industry, but the emphasis is primarily on public outreach and informational sessions. There does not seem to be any framework for contingency preparation exercises.

Recommendations

FBI/EMCS program

At the onset of my CCP, an enduring collaboration between the FBI and EMCS was my key deliverable. My proposal is that the FBI sends one or two employees to each subsequent cohort of Brown's EMCS. While there is nothing prohibiting an agent or member of the support staff from applying and attending EMCS at their own cost, most of those I interviewed about the program have stated that the financial cost and time commitment were too prohibitive to apply. Even if the cost of the program was not as big a factor, participation in each of the five residential sessions means that an employee is charged 200 hours of annual leave which takes the average employee over a year and a half to accumulate.

The general process of how a seat at an EMCS cohort would be filled involves five phases: advertising and application, screening and selection, cybersecurity familiarization and attendance. The advertising phase is the first step in this process during which the FBI would publish a memo, internally referred to as an Electronic Communiqué (EC), that announces that the application to the EMCS program is open and provides a description of the program and the eligibility requirements needed to attend. The timing of the advertising phase would coincide with the EMCS application window. According to the FBI program managers that oversee similar programs, eligibility requirements are likely to include a minimum time in service, a minimum performance appraisal of 'successful' or higher and being assigned to a cyber field. Participation in this program will almost certainly incur a two-year service extension agreement, meaning that enrollment would require the employee to remain in the FBI

at least two additional years or be held liable for the tuition. If an agent or analyst meets the criteria, he or she will be free to apply.

The second phase of the process is the screening and selection phase. Since I anticipate there would be an abundance of qualified candidates, the FBI would have to devise a selection process to pick the candidate the is most qualified to attend. The selection would be comprised of a review of the candidate's background and resume and the submission of some essays articulating how the candidate would leverage the contacts and knowledge to further cyber security initiatives in the FBI. A career board would convene to select the candidate and possible an alternate if the primary is not selected by EMCS.

To ensure that the selected attendee has a baseline understanding of the cybersecurity concepts that are introduced in the first residential session of EMCS, the cybersecurity familiarization phase will offer some classes via the Virtual Academy platform. These classes will cover the basics of cybersecurity and define common terms the attendee can expect to hear. During my first residential session, I remember having to compile a list of terms I had to look up and it seemed to me as if everyone else in the class understood the references.

The final phase of the EMCS program would be attendance. The experience and perspective that a member of the FBI would bring to the cohort would be extremely beneficial as my attendance and that of the FBI Agent in the third cohort have hopefully proven.

An FBI EMCS collaboration would also directly contribute to the problems in executive education I have outlined throughout this CCP. EMCS has given me unfettered access to some of the greatest minds in cybersecurity. The relationships I have developed with my peers will have a lasting impact on how I approach cybersecurity. Most importantly, EMCS has instilled the sense that cybersecurity must be approached from a multilateral and holistic perspective, one that I feel must become a part of the executive culture at the FBI.

Establishing a collaborative problem such as my FBI EMCS proposal faces some challenges. First, I have been advised that the cost of the program is prohibitive. The initial question I always faced when bringing the proposal to the attention of training unit managers is the cost. Brown's EMCS program is considerably more expensive than alternatives offered by other prestigious institutions such as Georgetown or the University of Maryland. Second, the program would have to be vetted by the Cyber Education and Training Unit (CETU). This step will not necessarily derail the program, but it will make

the proposal take longer. Finally, the program would have to allow attendees to schedule the residential sessions as training time and not annual leave.

Despite that a collaboration has not been delivered to date, the endeavor will continue after submission of this CCP. Next steps include discussing this proposal further with program managers and unit chiefs. In particular, the CETU will be engaged to establish the framework of the proposal and conduct a cost analysis.

Project Solarium 2.0

To develop a comprehensive strategy for the next decades in an ever-evolving cyber landscape, another of my recommendations is that senior members of the executive branch of government to conduct a national level exercise akin to the Project Solarium 'war game' that was conducted at the onset of the Cold War[25].

To address the looming threat of the Soviet Union in the wake of the Korean War, President Eisenhower developed a set a of policies which developed as a result of an exercise and process. The codename of this exercise was Project Solarium, named after the room in the White House that it was held in. It brought together three teams that were charged with arguing for a particular course of action to contain the expansion of the Soviet Union while furthering UN national interests. The teams and their assigned perspective was as follows:

"Task Force A was assigned to modify, with additional incentives, the Truman policy of containment. Task Force B was to delineate the perimeters of US security interests on the globe and announce that should the Soviet Union or its allies cross those lines, war would ensue. And Finally, Task Force C was to propose measures short of war-including political, economic, diplomatic and covert-to eliminate Soviet influence from the free world and weaken communist control in both Eastern Europe and in the Soviet Union itself."[26] One of the results of this exercise was the basis for a new national security policy for consideration by the National Security Council.

My proposed Project Solarium 2.0 would be in a cyber context and similarly pit three or more competing perspectives against each other. The goal of the exercise would be to devise the framework for a strategy on how to contend with the dire threats posed by China and Russia. In contrast to the original Project Solarium, this iteration would have to factor in several actors and a threat that is far less symmetric than that of the Soviet Union, whose aims and ambitions were well understood. I believe that such an exercise would only underscore the already apparent need for an agile-minded executive

body. The fact that the government will increasingly rely on public and corporate partnerships would also become abundantly apparent.

Changes to General and Executive Education

Rectifying some of the shortcomings identified in this CCP would have a tremendous impact on the FBI's cybersecurity posture and its ability to act as a force multiplier for private industry. Annual Infosec and Insider Threat awareness training would be more effective if there were some control measures that would do a better job of ensuring that the material is retained. Delinquency caused by neglecting to take the courses or failing them should instantly trigger the temporary loss of credentials. Access to case management systems should be contingent on having current Infosec and Insider Threat training certification.

Executive education should exploit the positive trend towards increased public engagement. I would recommend amplifying this collaborative spirit with public engagement that transcends the standard informational sessions and outreach that the FBI regularly conducts. One option is FBI sponsored war-gaming scenarios in which companies participate in cyber ranges such as the one offered by IBM[27]. Ideally, the FBI would set up cyber ranges of its own for public use.

Conclusion

Future conflicts will increasingly occur in the cyber domain which is becoming more complex with each new breakthrough technological innovation. Conventional intelligence collection methods are being gradually supplanted by cyber intrusion and some speculate that a cyber campaign will precede the onset of any major future war.

Future leaders of the organizations charged with protecting the United State's national security must evolve with emerging trends and capabilities. They must recognize the need to collaborate with technological innovators and with the companies that find themselves lucrative targets for intellectual property theft to jointly design defenses against the offensive cyber capabilities of China, Russia and many other adversaries the United States is beleaguered by.

References

1. Department of Justice, Office of Public Affairs, "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns". December 20, 2018 https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

2. Ibid

3. Alan Blinder, Nicole Perlroth, "A Cyberattack Hobbles Atlanta, and Security Experts Shudder" The New York Times, March 27, 2018. https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

4. Ellen Nakashima, Philip Rucker, "U.S. declares North Korea carried out massive WannaCry cyberattack", The Washington Post, December 19, 2017. https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html?noredirect=on&utm_term=.28eba21f6dd6

5. Department of Justice, Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage". May 19, 2014 https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

6. Ibid.

7. Dan McWhorter "Mandiant Exposes APT1 – One of China's Cyber Espionage Units & Releases 3,000 Indicators", Fireeye Threat Research, February 19, 2013. https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html

8. Jennifer Dlouhy, Michael Riley "Russian Hackers Attacking US Power Grid and Aviation, FBI Warns", Bloomberg, March 15, 2018. https://www.bloomberg.com/news/articles/2018-03-15/russian-hackers-attacking-u-s-power-grid-aviation-fbi-warns

9. Rebecca Smith, "Russian Hackers Reach US Utility Control Rooms, Homeland Security Officials Say", The Wall Street Journal, July 23, 2018. https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110

10. Ibid.

11. Joint Publication 3-13, Department of Defense https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

12. US Constitution, Cornell Law School, https://www.law.cornell.edu/constitution/fourth_amendment

13. US Department of Justice, Office of Justice Programs, Bureau of Justice Assistance https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1284

14. FBI Website, https://www.fbi.gov/services/operational-technology/going-dark

15. Ibid.

16. Ibid.

17. J. Freedom du Lac, Ellen Nakashima, "Tim Cook: US Government wants 'something we consider too dangerous to create'", The Washington Post, February 17. 2016 https://www.washingtonpost.com/news/post-nation/wp/2016/02/17/apple-ceo-the-u-s-government-wants-something-we-consider-too-dangerous-to-create/?utm_term=.0c3d878d95cb

18. US Office of Peronnel Management (OPM), Senior Executive Service, https://www.opm.gov/policy-data-oversight/senior-executive-service/

19. FBI Website, https://www.fbi.gov/about/leadership-and-structure/national-security-branch

20. FBI Website, https://www.fbi.gov/investigate/cyber

21. The National Strategy to Secure Cyberspace, February 2003, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

22. FBI Website, https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force

23. Ibid.

24. SANS, https://www.sans.org/

25. William B. Picket, "George F. Kennan and the Origins of Eisenhower's New Look: An Oral History of Project Solarium", Princeton Institute for International and Regional Studies, Princeton University, 2004 https://web.archive.org/web/20131029210208/http://www.rose-hulman.edu/~pickett/Solarium.pdf

26. Ibid.

27. IBM Security, X-Force Command, https://www.ibm.com/security/services/managed-security-services/security-operations-centers