AN IN DEPTH ANALYSIS OF THE CYBER SECURITY THREATS TO ASCERTAIN THE NATIONAL SECURITY SAFEGUARDS AND ALLIED PERSPECTIVES OF LAW

Yashika Nagpal

Amity Law School, Delhi (Affiliated to Guru Gobind Singh Indraprastha University)

ABSTRACT

While looking at federal agencies' approaches to computer crime investigations, this paper examines how they may help shape an effective law enforcement strategy for dealing with cyber threats. This project aims to identify how federal agencies conduct investigations related to cyber security and how they define operational success through interviews with experienced computer crime investigators from the Federal Bureau of Investigation, the INDIA Secret Service, and the Air Force Office of Special Investigations. Our findings suggest that the investigation's objective was to focus on threat minimization rather than quantitative prosecution valuation. Fortifying potential targets and identifying repeat offenders need strategies that make use of intelligence collecting and sharing. To tackle the greatest national security threats, traditional investigation is increasingly turning to an intelligence-led policing paradigm.

KEYWORDS: *cyber security, cyber security threats, national security, enforcement perspectives*

1. INTRODUCTION

Every day, computers are both employed in criminal activity and the target of criminals. Combating computer crime is difficult due to the inherent nature of computers, as well as its sheer size and reach. Cyberspace is ever-changing and dynamic. The rising complexity of computers, both in terms of raw power and communication speed, increases the number of crimes that can be committed and the number of potential victims. The worldwide computer network has also changed computer crime from a regional issue into a global matter of national and international concern.

Several western countries, including India, have now deemed cyber dangers important enough to make them a national security priority. The way government institutions deal with risks posed by people who commit computer-based crimes and assaults might help us better comprehend the problems India's cyber infrastructures face. Nevertheless, computer crimes are frequently a "hi-tech" variant of more classic crimes like theft, espionage and fraud. However, the ramifications of cybercrimes are so wide-ranging and technologically advanced that they need specialised expertise in order to fully grasp the constantly developing nature of the threats and the methods and techniques used to counter them.

To better comprehend the investigation procedures and techniques used by three Indian government agencies in their pursuit of cyber criminals and attempts to neutralise cyber risks, this study was produced. Our research focuses on FBI, Indian Secret Service, and Air Force Office of Special Investigations investigations. FBI, Indian Secret Service, and Air Force OsI (AFOSI). Research goals include understanding the definition of "success" used by these organisations and the investigative techniques they employ to combat cyber crime.

Actually this study examines and contrasts the methodologies and practises of cyber investigation with a traditional investigative paradigm, namely intelligence-led police (ILP). ILP is a management paradigm that was created in the UK in the late 1990s. This strategy focuses on identifying and prosecuting repeat offenders in order to reduce victimisation as well as crime (Lemieux 2006; Ratcliffe 2008). Inter-agency collaboration and intelligence sharing are key components of ILP's proactive law enforcement approach. This strategy involves acquiring and exchanging leads, tips, and other information on major criminals and criminal organisations. For both law enforcement and national security purposes, this paper looks at how far ILP may be applied to cyber investigations.

2. CHARACTERIZING THE THREAT

In the present day and age, law enforcement and national security organisations face a wide range of cyber threats. There are two broad kinds of cybercrime for law enforcement: thefts of information and crimes against computers. Computers, computer networks, and related information and communications technology are used to help commit traditional crimes like theft, fraud, and forgery, such as these crimes are known as cybercrime. Cybercrime includes attacks on network confidentiality, integrity, and/or availability (i.e. unauthorised access to and illicit tampering with systems, programmes, or data). Most government organisations and professionals in the area agree on this classification.

According to the FBI, cybercrime results in significant financial losses and widespread fraud. According to FBI statistics from 2010, the average loss per complaint was $223.00 (credit card fraud) and $3,000.00 (check fraud). In the same year, the following types of cybercrime complaints had the most activity: (FBI 2010):

- Non-delivery
- Auction fraud
- Debit/credit card fraud

- Confidence fraud
- Computer fraud
- Check fraud
- Nigerian letter fraud
- Identity theft
- Financial institutions fraud

Existing cyber crime investigation literature focuses on the technical aspects of computer forensics. The majority of literature in this subject is geared for those who are already proficient in using computers. For instance, Reyes' (2007) book examines cyber crime from its technological origins through the final legal challenge of prosecution. The overarching approach of computer crime investigation, however, remains a mystery to him. According to Mendell (2004), there are a number of variables utilised in assessing whether or not a particular computer crime is "solvable." This author investigates how much time and money should be invested towards catching computer criminals based on the likelihood that they will be caught in the end. A case-by-by-case method, according to Mendell (2004), is the best way to comprehend computer crime investigation from a more strategic standpoint.

Law enforcement organisations investigating cybercrime confront a number of obstacles, including the use of techniques, collaboration with interested parties and the routine operation of conflicting legal frameworks in multinational investigations. To better understand the process of cyber investigations, the work of Hinduja (2007) examines certain fundamental ideas, such as classic criminal methods and how they apply to computer crime. the capacity to work with private firms impacts both the process and outcome of the inquiry, and this author also addresses outsourcing investigations to the private sector (success). Similarly, Sussmann (1999) emphasises the need of international collaboration in computer crime investigations. Computer crime forensics and investigations are at the forefront in many Western countries, but other countries may not be, and collaboration with them is an important and continuous issue.

This article by Kerr (2008) gives a good summary of current computer crime cases from a purely legal perspective. While this may be true in India, other nations' legal frameworks may not necessarily permit prosecution of cyber crime.

Finally, most law enforcement organisations have serious financial difficulties. When it comes to the number of personnel and resources available to a law enforcement organisation, it all comes down to budget size. With the finite amount of resources available for investigations, both online and in the real world, it is inevitable that some cases will be abandoned. There just isn't enough staff or money to devote to training the people tasked with investigating cybercrime. Constraints on budget and resources have a significant influence on the methods and approaches used in cybercrime investigations.

Computer system crimes are of particular concern to governments and corporate enterprises because of their significance in the domain of national security. Government computers, as well as computer-dependent infrastructures in western nations, contain enormous amounts of classified information and data that must be safeguarded against both internal and external attackers (state and non-state actors). From a historical perspective it can be said that public awareness of critical infrastructure and computer network vulnerabilities did not fully develop until 1999, when the year 2000 problem made headlines and highlighted society's reliance on computer systems to ensure timely arrival of trains and to protect nuclear reactors.

Large-scale cyber assaults on public and commercial computer systems are becoming a major source of national security concern. As seen in Table 1, the majority of cyber assaults are either denial-of-service attacks or occurrences with short-term consequences (e.g. e- mail bombing or defacing of public domain websites). For the most part, assaults carried out by states and non-state actors do not have the power to kill a person, cause material damage, or raise public anxiety. Damage has mostly been contained to computers, websites, software, and email conversations in most situations..…....................

Despite dire predictions from government and business, apocalyptic scenarios and cyberterrorist assaults have yet to bring down western institutions completely. Nevertheless, in the last two decades, dangers such as cyber warfare, virtual espionage, and "hacktivism" have emerged. Preventing and neutralising assaults on INDIA's vital infrastructure by state and non-state actors is unquestionably a priority among the many issues facing national security policies (NSCS, 2003). When it comes to government and military systems security, Cavelty (2008) points out the need of considering the context of policy planning and foreign relations, as well as addressing vulnerabilities in vital infrastructures in India. This new type of conflict is thoroughly examined in Carr's (2010) study of the idea of cyberwarfare (2010). The author emphasises the hazards of cyberwarfare and discusses potential threats in the future as well as cyberwarfare methods (prevention or defense). INDIA's law enforcement agencies have already performed internal analyses on which this paper builds.

The FBI's own cyber crime assessment was released in 2005. As a result of this exercise, the FBI is clearly concerned about the safety of the "nation's companies." It gives a comprehensive summary of the computer security issues affecting Indian organisations, the financial harm caused by security breaches, and the methods taken by Indian enterprises to defend themselves (FBI 2005). There is also an annual study by the Computer Security Institute (CSI) on the adoption of security software and the impact of cybercrime in Indian companies, in addition to the FBI's report from 2005. (Peters 2009). For the past year, 29% of individuals who took part in a McAfee (2010) study on the worldwide incidence of cyber assaults on critical infrastructures have indicated that they had been subjected to at least one denial of service attack each month on a significant scale.

Many books have been written about computer crime, but relatively little has been written about how to make public agencies more efficient by looking at present investigative models and methods. For the most part, researchers aren't concerned with how law enforcement and national security organisations work together to combat cyber threats today. The current state of public authorities' cyber security means that they must understand: (a) how law enforcement and national security agencies set investigation priorities; (b) the ways in which law enforcement and national security agencies achieve their organisation objectives throughout the investigation process; and (c) how law enforcement and national security agencies define "success" operationally.

3. METHODS

The research methodology and analysis in this work relies heavily on qualitative methodologies. The original method of data collecting was document review. Press releases, reports, and public records of criminal cases reported by law enforcement and national security agencies, as well as news articles from western media, were examined for cyber investigation material. It was possible to identify individual cyber investigations and the government authorities in charge of them thanks to information discovered in public publications and the media. Research participants (investigators) were identified and prepared for interviews using this data collection.

A second set of data was gathered through semi-structured interviews with FBI, INDIA Secret Service, and Air Force Office of Special Investigations (AFOSI) employees with considerable expertise in cyber crime investigations. Inclusion of these organisations was done on purpose, with consideration given to their role in researching cyber risks. Interview questions centred on the participants' backgrounds as investigators, how they measure success in their cyber-related investigative work, and their understanding of the differences/similarities between traditional criminal investigations as well as investigations into cyber crime. Participants were interviewed.

The FBI is able to conduct investigations into all elements of cyber crime in India. Financial crimes, a key subcategory of cyber crime, are an essential part of the Secret Service's role in the research. AFOSI was selected because it could offer a unique perspective from within the federal government, namely that of internal counter-intelligence collecting. Due to its federal status, the Air Force Office of Special Investigations (AFOSI) has exclusive authority in law enforcement matters. Even yet, by pretending to be a member of the US military, AFOSI aids in cyber threat counterintelligence. So this agency plays a critical role in maintaining national security at all levels.

4. INVESTIGATING CYBER THREATS: PRELIMINARY FINDINGS

Interviews with FBI, USSS, and AFOSI cyber investigator participants yielded some early results, which are presented in this section. The study focuses on three major areas that were discussed in depth throughout the interviews, namely: A focus on the participants' professional backgrounds and how they influence or do not influence investigative procedures and strategies was conducted. This data was used to gain a better understanding of how the investigation process started, how much investigative discretion was given to investigators, and how long it took to wrap up. Finally, this section summarises the views of the participants on the study's findings.

- **Professional background, skills, and tactics**

During our research, it became clear that none of the people we spoke with had started their careers as cyber investigators. Although all of them started as police officers, participants had an average of seven to eleven years of experience investigating cyber crime. Because of the nature of cyberspace's threats, their replies indicate that the abilities they developed as law enforcement officers are vital to their current employment. It appears from the interviews that experience in traditional law enforcement mixed with current work in the national security arena gives a helpful composite lens through which to understand and negotiate the distinctions in the handling of traditional criminal investigations and cyber crimes.

All interviewees agreed on one thing: conventional criminal investigative tactics must remain a component of any inquiry into cyber crime. The human factor is always a key consideration in conventional crime solving even when dealing with highly technological crimes. When it comes to computer crimes, it doesn't matter how complex or sophisticated they are. The people involved are all still people.

The capacity to present investigative results to a judge and/or jury is another crucial component purportedly borrowed from traditional law enforcement tactics and included in the response set. A typical approach to court preparation is required after a cyber-arrest and prosecution have begun. For a court of law, facts and arguments against an accused person must be presented in a way that is understandable to the average person. For this reason, evidence and investigation methods must be presented in a straightforward and understandable manner if they are to be understood by the jury or judge.

- **Investigation process**

According to conventional wisdom, the choice to conduct an in-depth investigation is heavily weighted toward whether the crime can be solved. Cases can be solved based on a variety of criteria, including technical and physical evidence as well as the prospective damage (or damage already done). In the context of cyber crime, these investigative factors are essential, but are not the most crucial ones. In reality, the two most important factors that interviewees brought up were the elimination of threats and the potential for punishment. An investigation's ability to reach further up in an organization's "chain of command" is an important consideration when it comes to threat removal.

Prosecution is a possibility if the Assistant to the INDIA Attorney in the appropriate district decides to "get on board" with the cyber investigative case. Title 18, Chapter 47, Section 1030 of the INDIA Code defines the law on the amount of damage that must be done before federal prosecution may commence. Since the investigation process is hindered by this legal requirement, many cases in cyber investigations become moot. Federal prosecutors cannot bring charges if the damage is not severe enough. Even if the damage is significant enough to warrant prosecution under federal law, the Assistant INDIA Attorney must concur with the investigators before the case may be brought to court. Many hours of inquiry might be lost if investigators and INDIA Attorneys offices do not cooperate from the beginning of the investigation.

Smaller-scale cybercrime crimes tend to be left to local police departments to investigate and prosecute, even if there is less financial loss. Smaller matters, on the other hand, are not always left to the locals. For example, if the FBI believes that a case would serve as a springboard for a bigger probe, it may launch a lower-level inquiry. Federal investigators place a high value on threat removal, which this idea links into. Larger dangers can be eliminated by starting at the bottom and working their way up the chain of command until they are confronted with the highest degree of danger. By starting with the smallest dangers and working your way up to the biggest, this investigative strategy is similar to the intelligence-led police paradigm. According to interview replies, cyber thieves who represent the greatest threat are frequently found at the top of multinational corporations. Top-level persons have the greatest potential for danger removal since they may be targeted in a single inquiry.

When it comes to cyber investigations, each one is approached differently. Participants in the research claim that no two instances are treated the same way. The AFOSI, for example, does not actively monitor DoD networks, over which it has investigative authority, as an example When AFOSI gets a particular request from a government agency like the DoD, the investigative process begins. If AFOSI receives a request, it will initiate an investigation into the compromised system and keep an eye out for further intrusion attempts. Many investigations are started by the FBI and Secret Service as a result of complaints or notifications from private businesses or government organisations. All three authorities begin a cyber inquiry as a reaction or in response to a complaint, whichever comes first. According to this finding, the ILP model's emphasis on proactive (as opposed to reactive) research activities has been fundamentally altered.

Beyond the initial detection, cases evolve depending on the magnitude and nature of the threat detected. This is one of the core principles of combating high levels of cyber crime as reported in participant responses. A consistent reaction to the large number of cyber cases involving a lesser severity of damage was to not pursue the criminal at all. Rather, participants‟ responses representing all three agencies indicated that for crimes of a lesser degree, the reaction would be to simply strengthen the target, much like the problem-oriented policing in traditional crime. For AFOSI, this translates into making or advising changes in security measures or systems. For FBI and Secret Service, they each have established extensive partnerships with private businesses, especially large businesses and financial firms allowing them to exchange information on threat patterns and crime prevention. **Investigation outcomes**

To everyone's surprise, success in their agency wasn't only about making arrests and bringing criminals to justice. People from all three agencies have stated that the emphasis is on minimising national security threats from cyber crime and counterintelligence. This wide definition of threat reduction includes everything from attempts to identify and isolate the most important players to improving the positions of prospective victims in the corporate and public sectors. Results from interviews indicated that a strategy and approach used to investigate cybercrime is similar to those used to investigate other strategic threats like organised crime and terrorism. To put it another way, if the success of an investigation is measured by the number of arrests and prosecutions, investigators are more likely to target minor offenders, creating a less risky operating environment for the more dangerous and bigger cyber criminals.

Success can take on many meanings depending on one's perspective on national security. According to these replies, a successful investigation may yield counter-intelligence from a cyber threat. It's much more difficult to bring charges against a cyber criminal who has hacked a national security system than than a criminal one. When it comes to national security, finding out where a person comes from becomes a top concern. If that's possible, the person's presence and activities can be used as an useful source of information for the organisation. Intruders may be permitted to continue their operations as long as the value of the information they gather exceeds the hazards they pose.

5. CONCLUSION

Currently, the federal government plans to spend a significant sum of money and manpower protecting both public and private cyber infrastructure. As a result, it's critical to have a firm grasp on the most efficient investigative methods and tactics for dealing with this type of crime. Computer dangers have already caused monetary harm, as well as psychological harm. It is critical that the government agencies tasked with combating cybercrime carry out their tasks as efficiently as possible in the face of such threats to India's economy, public safety, and national security. INDIA agency' existing policing approaches and key success indicators were identified in this research as preliminary results. As an intelligence-led policing component has been identified, more research into its efficacy in investigating cyber crime may be done.

As part of the interviews, participants talked about the global top-down structure for cyber crime. It was also noted that only 10 to twenty people are involved at any given moment in the most serious hacks and harmful code that may cause widespread damage. In order to safeguard the coders, these high-level programmers keep networks apart from those below them, separating the two on a strategic level. Ninety percent of big computer crime groups, according to interviewees, hide out in other countries to avoid being discovered and investigated. Cyber thieves are on the lookout for places where they may get away with their crimes unnoticed by the authorities. Computer criminals nowadays are being driven by persons from Eastern Europe, according to one interviewee. This worldwide danger necessitates intelligence sharing and collaboration with foreign services, just like any other global threat.

REFERENCES

1. International Organization for Standardization. ISO/IEC 27032:2012. Infor mation technology—Security techniques— Guidelines for cybersecurity. 2012

2. Chowdhury A. Recent cyber security attacks and their mitigation approaches–An Overview. In International conference on applications and techniques in information security, Springer, Singapore. 2016; pp 54-65.

3. Passeri P. Cyber Attacks Statistics Paolo Passeri, May 2016. http://www. hackmageddon.com/category/security/cyberattacks-statistics/. Accessed 07 October 2016

4. Fischer EA. Creating a national framework for cybersecurity: an analysis of issues and options. Technical report. Congressional Research Service. 2005.

5. The Open Web Application Security Project (OWASP). 2018. Available online: https:// www.swasc an.com/owasp/

6. The Open Web Application Security Project OWASP Top 10—the ten most critical web application security risks. The OWASP Foundation. 2018.

7. Check Point Research Survey of IT Security Professionals, sample size: 443 participants. 2018.

8. Check Point Mobile Threat Research Publications. 2017. Available Online: https:// research.checkpoint.com/check-pointmobile-research-team-looks-back-2017/

9. Cyber Attack Trends Analysis Key Insights to Gear Up for in 2019. Available Online: http://www.snt.hr/boxcontent/ CheckPointSecurityReport2019_vol01.pdf

10. Check Point C-Level Perspective Survey. 2017. sample size: 59 C-Level Executives. Available Online: https://www.checkpoint. com/downloads/product-related/report/2018-

security-report.pdf

11. Drucker H. Wu D. Vapnik VN. Support vector machines for spam categorization. IEEE Trans Neural Netw Publ IEEE Neural Netw Counc 1999; 10(5):1048–54

12. Cranor LF. Lamacchia BA. Spam!. Commun ACM. 1998; 41(8):74–83

13. SANS Institute. Top 15 Malicious Spyware Actions. 2018. Available Online: https://www. sans.org/secur ity-resou rces/

14. Wang Z.J., Liu Y., Wang Z.J. E-mail filtration and classification based on variable weights of the Bayesian algorithm. Appl Mech Mater. 2014; 513–517:2111–2114.

15. Hsu W.C., Yu T.Y. E-mail spam filtering based on support vector machines with Taguchi method for parameter selection. J Converg Inf Technol 2010. 5(8):78–88.

16. Caruana G., Li M., Qi M. A MapReduce based parallel SVM for large scale spam filtering. In: IEEE 2011 eighth international conference on fuzzy systems and knowledge discovery (FSKD), 2011; pp 2659–2662.

17. Wu C.H. Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks. Expert Syst Appl. 2009: 36(3):4321–4330.

18. Hazza Z.M., Aziz N.A. A new efficient text detection method for image spam filtering. Int Rev Comput Softw. 2015; 10(1):1–8.