Strategies to Detect, Apprehend, and Prosecute Malicious Attackers

Ashok Kumar Reddy Nadikattu

Sr. Data Scientist & Department of Information Technology

California USA

Abstract

Like all other nations of the world, the frequency of cybercrime in the United States of America (U.S.A.) increases over time. However, due to the rise of online activities and global connectivity, cybercrime is spreading rapidly in a terrific volume has become an international matter and not a territorial one. Generally, by law, crime can be defined as a territorial phenomenon in how the law is territorial (Lucas, 2017). However, the issue has become a global matter and not necessarily a territorial one. Recently, America has been in the surge of cybercrimes. Various attacks have been made in multiple sectors. Even though the country has been trying to develop tactics to prevent these attacks, the strategies have not been effective. By assessing the various gaps in the country's law enforcement policies and the rise in cybercrimes in the country, this paper intends to present a foundational of the cyber compliance strategies; the paper will define the issue and present areas that need policy solutions in the future. Thus, this paper sets the groundwork for effective prosecutions of attackers and numerous methods for constructing a more comprehensive security compliance infrastructure.

Keywords

Cybercrime, cybersecurity laws, malicious cyber actors

Introduction

To conduct multistage, multijurisdictional attacks, malicious actors take advantage of technological vulnerabilities and international cybersecurity cooperation. The consequences will vary from inconvenience to complete devastation. States, organizations, state-sponsored organizations, or cyber actors engage in deliberate attacks with the aim of infiltrating and altering computer instructions. In the past, the US has encountered adversarial states and militant non-state parties grouped in vertical institutions that were relatively hierarchical (Garcia, 2018). However, thanks to the advancement of intelligence, US adversaries can now be classified as a horizontal network of dispersed leadership and no direct signs of state power.

Because of the persistence and complexity of cyber-attacks, many strategic interventions for cybersecurity in critical infrastructure defense have been established, including a cybersecurity architecture, knowledge exchange systems, and other cyber tactics. Across the globe, several nations have adopted common strategies. While many countries are implementing advanced cybersecurity policies, they remain fragile, and most countries around the world have restricted cyber-response ability. Several recent studies and well-publicized corporate investigations have linked several attacks against US commercial infrastructures to China, following malicious data being pivoted across a variety of servers. (Segal, 2017). Although plans for responding to cyber-attacks in the United States are still being established, attempts should be taken to put measures in place to detect, pursue, and prosecute disruptive cyber actors. Instead of putting cyber criminals in the center of attention of America's cybersecurity programs, the government should elevate the costs of their actions in order to bring cyber actors to account and deter future assaults.

Literature Review

The Rise in Cybercrime

Cybercriminals come in a variety of sizes and forms. Cybercrime is an illegal activity that involves a computer, networked device, or a network committed by hackers or cybercriminals to generate profit in the form of gaining money. According to the FBI, these attacks may come from a variety of actors with a variety of motives and affiliations (Padda, 2016). According to Gupta, lone attacked operate mid-level identity fraud for financial gain. Lone actors with malicious political or personal reasons often commit crimes such as doxing (2018). On the other hand, High-level actors typically branch from cyber actors associated with state-sponsored actors or crime syndicates.

The rate at which often unseen crime is occurring in America is rising rapidly. Pazik (2017) stated that, in 2016, the number of self-reported cybe\rcrime cases received by the Federal Bureau of Investigation (F.B.I.) through its Internet Crime Complaint Centre was about 298,728 (Eoyang et al., n.d). Many of the cases presented to the F.B.I. could credibly be described as systematic cyber breaches, ransomware, malware, and personal data breach. Surprisingly, Eoyang et al. (n.d) argue that the F.B.I. estimates that only 15% of the crime are reported by fraud victims nationwide. This implies that there is 2 million cybercrime per year nationwide. Terrorists have been using the internet as a primary tool to perform destructive cyber-attacks against US government (Broadhurst, 2018). Many of these offences endanger the integrity of institutions, either deliberately or by the manner in which they expand.

Cybercrime affects a large number of citizens in the United States, in all states, territories, and various sectors. Due to other cybersecurity laws, demographics, and corporate representation in several states, the states experience the highest number of victims, which leads to economic losses to the rise in the cybercrime rate. Besides bearing the weak security incidences and data braches, malicious cyber actors are hitting various sectors such as health care, manufacturing, accommodation, and the public. For example, Zhang et al. (2016) claim that after an attack on the Mirai Botnet in 2016, some of the world's most well-known domains became unavailable for up to twelve hours, costing businesses millions of dollars in missed revenue. In addition, cyber criminals have targeted sensitive facilities and healthcare services in the United States. Many lives, infrastructure, and large-scale damage would be lost if these structures were successfully attacked.

The Compliance Deficit

It is more difficult to investigate the adequacy of the solution to cybercrime concerns. Not only is the US government dealing with a high incidence of cybercrime, but it is now dealing with a secret compliance crisis. Garcia (2018) claims that America's compliance deficit has been widely obscured due to insufficient metrics for investigating law enforcement response. Standard crime rates still don't account for the new types of offences that are taking place today. Furthermore, because of the lack of consistency in investigating incidents, state, municipal, and federal authorities do not investigate cybercrimes in a coherent or transparent approach.

The proportion of reported crimes is proportionally diminutive as compared to the number of actual crime rates. Considering that cybercrime victims rarely report cases, Eoyang et al. (n.d) indicate that the effective law implementation rate estimate may be close to 0.05%. However, Eoyang et al.also that the F.B.I. database suggests that the estimated enforcement rate for reported incidents is 0.3 % (n.d). While the case such as internet fraud is minimal, they are essential and meaningful in punishing cyber actors contributing to a small, large bucket. However, given the unlikelihood of being subjected to the law and the increase in ease of committing these crimes, it's without a doubt that various cybercrime is on the rise.

The lack of a firm law enforcement policy in cybercrime needs to be urgently addressed. The problem is visible in many countries and has an effect on many people's lives, but politicians are insensitive to it (Negron, 2018). In any other domain, aggressive attackers' lack of intervention and perceived immunity will not be accepted. However, in the context of cybercrime, it is often seen as an afterthought. This is a crucial component of introducing a regulatory approach that can catalyze behavioral change.

However, if the cyber criminals are working in the best interest of nation-states to accomplish their objectives by cyber-attacks, it would be far more difficult to prosecute or alter their actions. Besides, according to Garcia (2018), the foreign government sponsor is likely to recruit others to pick up the flag and resume the attacks in case the one sanction or arrests them. Thus, many need greater coordination to organize attempts to bring punitive measures against the perpetrators, coordinating with the states that prohibit attacks. However, if the state resists or aids the attacker, political pressure can be applied to persuade the foreign state to change its stance about its role in the attacks. Suppose the state is directly responsible for the attacks and that the attacking state facilitates or carries them out as part of its foreign policy. In that situation, the victimized nation would need to consider all of its choices, including law enforcement and diplomacy.

Notably, just because several nation-states are employing cyber-attacks as a tool to achieve their goals does not mean the U.S. should disregard the considerable cybercrime surge that is sweeping the globe, giving immunity to the vast number of disruptive attackers who could be detected, thwarted, and punished (Greer, 2017). If the action results from an individual's or a government's decision, whether the fingerprints on the keys or the ones authorizing the warrant, it is still the person whose judgment has been influenced that should suffer the actual repercussions.

Reevaluating the United States' Approach to Cybercrime

Given the size of the cybercrime surge and the compliance vacuum that the country is experiencing, it's clear that the new method is inadequate. The number and severity of cyber-attacks have grown, comprehensive cybersecurity efforts have been critical, but not nearly enough. The infinite number of vulnerabilities and a developing number of attacks give rise to a finite number of cyber actors. However, to end these attackers, the government should change its perspective on cybersecurity and reevaluate its policies to concentrate on pursuing cybercriminals significantly.

The government is the sole agency with the power to intervene in the human attacker's case and the right to prosecute them. Under the Obama and Trump administrations, there has been an increasing focus on going after disruptive cybercriminals by law execution measures and introducing other forms of repercussions such as law enforcement actions to alter their behavior (White, 2016). However, as the compliance rate demonstrates, these measures are insufficient. They haven't been adequately resourced, and they haven't been offered the political support they need to move forward.

The U.S. government has put a high priority on defending systems and network security. A blame-the-victim culture in cybersecurity has contributed to this strategy. Thus, designing more robust firewalls against hacks, designing improved keys codes, and training users are crucial. However, a technique based solely on erecting impenetrable cyber barriers and human users incapable of making mistakes will fail. Policymakers should develop a more comprehensive parallel effort for identifying, stopping, and punishing cyber actors. By balancing system defense with an offense designed to control and discourage malicious cyber actors, they will alter the paradigm of malicious cyber attackers.

Corporations in the United States are concerned with the financial and reputational consequences of a major hack, thus they concentration their determinations on securing their networks and private information. However, when a big data attack occurs, , an organization is often dragged before Congress and made to apologize for its mistakes, technological shortcomings, and failure to have the most up-to-date security measures (Tran, 2018). Some of these businesses should be chastised for failing to take enough measures. Equifax, a financial reporting service that stores millions of Americans' records, was compromised in 2017 due to their failure to upgrade their applications after learning about the possibility for months (Berghel, 2017). As a result, according to Berghel (2017), hackers could take advantage of the situation, revealing the personal information of 143 million Americans. This should have been avoided, and businesses that refuse to patch identified flaws should be held responsible.

In parallel to the private sector, the government has largely taken a defensive approach to cybersecurity. The Comprehensive National Cybersecurity Initiative (CNCI) was developed by the Bush Administration in 2008, was a practical approach to internet security. It developed a comprehensive sequence of strategies aimed at safeguarding the US in cyberspace. It was a call to arms for the government to develop and modernize its position in network defense, knowledge sharing, and cyber-education. While the approach is a vital plan for bolstering law administration endeavors at home and overseas, as well as imposing sanctions on cyber criminals and nation-state sponsors, it also focuses primarily on cybersecurity, with just a very brief part dedicated to prosecuting hackers.

When explaining how the government combats hackers, military language is sometimes used, which is inapplicable to the majority of today's attackers. Several attempts have been prepared to describe cyberwar rules and establish Digital Geneva Conventions (Tran, 2018). After the devastating Russian counterstatement of service attacks on Estonia in 2007, military authorities have questioned whether a cyber-attack is serious enough to be deemed a war crime. Given the large amount of military expenses on cybersecurity, and the over-militarization of US foreign policy in general, it's no wonder that the issue about whether or not a cyber-attack would result in a tactical response has sparked heated discussion.

Cyber arms could not be the safest choice in a particular scenario due to various risks and attackers. This is due to the fact that military are cannot actively engage the cyber assailant since they are restricted to cyberspace (Kumar et al., 2016). Rather than using direct coercion, the government can utilize its Title XVII authority to concentrate law implementation on the offender at any time (Kumar et al., 2016). Regrettably, existing priorities undervalue and underinvest in the answer. Only by reforming law enforcement, with the help of diplomacy, may the government combat this cybercrime surge and close the cyber compliance deficit.

Recommendations

America, which lacks a robust cybersecurity policy to detect, prevent, and prosecute cybercriminals, is in desperate need of one. This approach would include domestic and international elements and the necessary framework and mechanism to achieve its goals.

For a change the government to change compliance activities, it must fix cybersecurity workforce constraints and how the workforce is educated, incentivized, and maintained to track down and apprehend cybercriminals (Dawson, 2016). The cybersecurity positions shortage affects both the private and public sectors, with openings ranging from information technology (I.T.) professionals to law enforcement cyber investigators. The large amount of job vacancies has a negative impact on the government's and corporations' attempts to ameliorate their cybersecurity, and law administration's ability to track down cyber actors. Furthermore, the significant shortage of equity in this sector, which could significantly improve the efficiency of the workforce, has a negative effect.

One of the most pressing challenges facing the U.S. government is finding qualified cyber talent, which has had a significant effect on U.S. law enforcement agencies. As a result, there is a need to raise pay for cybersecurity specialists, including those who work for the National Cyber Investigation Joint Task Force in cyber investigation positions. Moreover, it is still difficult to ensure that law enforcement officers are adequately prepared to perform cyber investigations. To train law enforcement agents to deal with hacking accidents, multiple specialties, such as detectives who investigate cases and specialized forensic experts who research automated gadgets and fingerprints, as well as first responders who protect crime scenes, will need to improve their technical capabilities (Tran, 2018). The way law enforcement agents are prepared to deal with digital forensics with these types of cases will have to adjust dramatically.

Many in the cybersecurity community have concluded that regulatory efforts would have little impact on America's enemies who use cyber-attacks to target the nation. However, even in the most daunting situations, regulatory measures taken against disruptive cybercriminals may significantly affect. In times of harmony, law enforcement is how the government negotiates with those who have violated the rules. Recent high-profile compliance actions show what can be accomplished as criminal justice system and diplomats concentrate on individual attackers and collaborate on a plan of action. For instance, following a sequence of cyber attacks on intellectual property in the private sector in the United States, the Obama administration placed diplomatic pressure on China in 2015. The Chinese government detained individuals convicted of cyber economic espionage under threat of sanctions. In cybercrime cases, indictments and convictions are potent tools (Segal, 2017). Victims are entitled to justice for the crimes committed against them. However, simply bringing indictments and leaving the hackers free in foreign lands is insufficient. The end aim is to remove them from the game entirely, and law enforcement, aided by diplomats, accomplishes this.

Not only does law enforcement need to change itself on a domestic level, but it also has to transform how it operates across international boundaries. Since the cyber challenge is global, the US government must have committed and deliberate leadership and planning at the highest levels in order to improve international collaboration and cooperation in closing the law implementation gap. Given the number of countries threatened by cybercrime investigations, if America's cyber diplomacy and compliance programs are not increased, and bilateral relations with allied nations across the world are not improved, only a small improvement would be noticeable. The U.S. government needs overseas cybercriminals to be apprehended. To apprehend foreign cybercriminals, the U.S. government requires a concerted international initiative, cooperation in constructing the prosecution, and collaboration in apprehending the offenders.

Conclusions

To transform the U.S. government's capacity to detect, deter, and discipline cyber attackers, the government needs a plan that focuses on finding actors rather than just creating better security. Cybercrime continues to be widespread, and the U.S. government's attempts to combat it must be as productive and successful as possible. This would require essential changes to de-conflict the various U.S. government departments participating in enforcement's frequently conflicting mandates. The emphasis of reforms should be on de-conflicting the departments in charge of cyber regulation, focusing on streamlining efforts, reducing redundancy, and clarifying authority. The U.S. government must review and extend its funding for global cyber enforcement capacity building to improve the capabilities of partner countries. It must assist international policymakers in comprehending and dealing with the challenge as it evolves. A thorough review of existing government activities in all departments involved with cybersecurity must be conducted to ascertain what is progressing, what needs to be amplified, and what needs to be changed to continue improving the government's capacity to prosecute cybercriminals. The U.S. government must review and extend its funding for global cyber enforcement capacity building to enhance the capabilities of partner countries. It must assist international policymakers in comprehending and dealing with the challenge as it evolves.

References

1. Berghel, H. (2017). Equifax and the latest round of identity theft roulette. *Computer*, *50*(12), 72-76.
2. Broadhurst, R., Lord, D., Maxim, D., Woodford-Smith, H., Johnston, C., Chung, H. W., & Sabol, B. (2018). Malware trends on 'darknet'crypto-markets: Research review. *Available at SSRN 3226758*.
3. Dawson, C. (2016). Law enforcement and the'attribution problem'in cyberspace. *Journal of the Australian Institute of Professional Intelligence Officers*, *24*(2), 32-42.
4. Eoyang, M., Peters, A., Mehta, I., & Gaskew, B. TO CATCH A HACKER.
5. Garcia, N. (2018). *The use of criminal profiling in cybercrime investigations* (Doctoral dissertation, Master's Thesis). Available from ProQuest Dissertations & Theses Global database.(Accession Order No. AAT 10839020)).
6. Greer, B. (2017). The Growth of Cybercrime in the United States. *Growth*.
7. Gupta, A. (2018). The evolution of fraud: ethical implications in the age of largescale data breaches and widespread artificial intelligence solutions deployment. *International Telecommunication Union Journal*, *1*, 0-7.
8. Kumar, S., Benigni, M., & Carley, K. M. (2016, September). The impact of US cyber policies on cyber-attacks trend. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)* (pp. 181-186). IEEE.
9. Lucas, G. R. (2017). *Ethics and cyber warfare: the quest for responsible security in the age of digital warfare*. Oxford university press.
10. Negron, G. L. (2018). *Social Engineering: How Cybercriminals Hack the Human Psyche* (Doctoral dissertation, Utica College).
11. Padda, E. S., Gupta, E. S., Apoorva, E., Lofty, E., & Kaur, E. A. (2016). Honeypot: A security tool in intrusion detection. *International Journal of Advanced Engineering, Management and Science*, *2*(5), 239437.
12. Pazik, E. (2017). *Ransomware: Attack Vectors, Mitigation and Recovery* (Doctoral dissertation, Utica College).
13. Sapienza, A., Ernala, S. K., Bessi, A., Lerman, K., & Ferrara, E. (2018, April). Discover: Mining online chatter for emerging cyber threats. In *Companion Proceedings of the The Web Conference 2018* (pp. 983-990).

14. Segal, A. (2017). Chinese cyber diplomacy in a new era of uncertainty. *Hoover Institution, Aegis Paper Series*, *1703*, 1-23.
15. Tran, D. (2018). The law of attribution: Rules for attribution the source of a cyber-attack. *Yale JL & Tech.*, *20*, 376.
16. White, J. (2016). Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies. *Global Security Studies*, *7*(4).
17. Zhang, J., Zhang, R., Zhang, Y., & Yan, G. (2016). The rise of social botnets: Attacks and countermeasures. *IEEE Transactions on Dependable and Secure Computing*, *15*(6), 1068-1082.