

UNVEILING THE GLOBAL IMPACT OF CYBERCRIME



Dr./ Toumi Nour Elhouda ^{1,2}, Dr./ Soualhia Imad ^{3,4}

¹ University of Lancaster, (UK)

² & Senior Lecturer B. University of El Oued, (Algeria)

³ University of El Oued, (Algeria)

⁴ Corresponding Author: soualhia1200@yahoo.com

Date of submission: 05/04/2024 Date of acceptance: 24/04/2024 Date of publication: 28/04/2024



Revision of the article: Dr./ Zerara Saidia (Univ. of Algiers 2)

Abstract:

Cybercrime poses a significant and growing threat to computer networks' security, prompting governments, police departments, and intelligence units worldwide to take action. Police forces around the globe have established dedicated cyber units and have begun training their personnel to combat this menace. Accordingly, this study aims to shed light on cybercrime by exploring its various types and providing relevant examples

Key words: Cybercrime; Threat; Protection Hacking; Cyber cells.

Introduction:

Cybercrime encompasses a spectrum of illicit activities involving computer networks or interconnected systems. While many cybercrimes are driven by financial motives, not all can be classified as such. Some perpetrators of cybercrime are sophisticated and well-organized, while others are newcomers exploring the world of hacking.

These crimes include cyber cracking and denial-of-service attacks, where computers or networks are either used as a weapon, a target, or a platform for illegal activities. In the realm of national security, cybercrime can take on various forms, including lobbying, espionage, and information warfare.

The management of cybercrime security has become imperative for national security, military-related scientific security, and intelligence management. It necessitates the development of a comprehensive policy to delineate the roles and responsibilities of various entities within a connected framework. The scope of

addressing cybercrimes varies widely, underscoring the complexity of this issue on an international scale.

This study aims to offer a conceptual framework for comprehending cybercrime and recognize it as a global challenge that demands thoughtful consideration and proactive measures. Accordingly, it attempts to answer the following research questions:

RQ1: How can the diverse security challenges posed by cybercrimes be identified and addressed at the national security level?

RQ2: How can a comprehensive policy framework be developed to confront these challenges both nationally and internationally?

To answer these questions, the following hypothesis was adopted:
Hypothesis: To address cybersecurity challenges, it is hypothesized that implementing transparent and accountable governance models is essential. This includes establishing robust control mechanisms over political authorities to rebuild trust between citizens and governmental institutions.

Methodology: The study utilized an analytical approach to analyze cybersecurity challenges and policies. It also involved examining annual reports from the European Ombudsman Foundation. This methodology was deemed suitable for conducting legal and political research, allowing for a comprehensive understanding of the topic.

In order to address the research questions and test the validity of the hypothesis, we suggest a framework consisting of four main parts:

- 1- Cyber Stalking.
- 2- Hacking.
- 3- Cybercrime Examples.
- 4- The future of cybercrime.

THE FIRST TOPIC:

Cyber Stalking

Cyberstalking is a form of online harassment where individuals use the internet or other electronic means to stalk, harass, or threaten someone. It can involve sending threatening emails, messages, or posting personal information online with the intent to harm or intimidate. Cyberstalking can have serious consequences for victims, including emotional distress and invasion of privacy. Laws and regulations regarding cyberstalking vary by jurisdiction, but it is generally considered a criminal offense.

The first requirement: understanding the complexities of cyber stalking

Cyber stalking involves using coercion, shame, and harassment to control the victim, often with the goal of financial gain, such as emptying bank accounts or damaging credit scores. This form of stalking aims to isolate the victim by targeting their family, friends, and workplace. Cyber stalking can manifest in various ways, including online harassment via social media, forums, or email; it is typically a sustained and organized effort over time (Pittaro, 2007, p. 183).

Initial encounters in cyber stalking cases may appear harmless, with odd or unsettling incidents occurring sporadically, especially in the beginning (Bocij, 2004, p. 188); this phase often involves the stalker gathering information and testing boundaries to assess the victim's reaction and vulnerability. As the stalking progresses, the behavior may escalate to more intrusive and threatening actions.

The term "tech stalker" describes a stalker who uses technology to monitor their target's activities and movements; this can include checking their target's social media updates to track their whereabouts, monitoring their online communications, or using GPS tracking devices to physically follow them. Tech stalkers often use a combination of online and offline tactics to harass and intimidate their victims, blurring the lines between physical and digital stalking.

The second requirement: legal ramifications of cyber stalking

Tracking down and prosecuting professional cyber stalkers is challenging due to their adeptness at concealing their identities. Additionally, many countries lack stringent legislation specifically targeting cyber stalking. In the United States, cyber stalking is addressed under harassment and anti-stalking laws, with penalties ranging from fines to imprisonment based on the severity of the offense.

The Violence Against Women Act (VAWA) in the United States specifically includes provisions addressing cyber stalking. However, federal laws targeting stalking through electronic means are lacking, and most legislation is enacted at the state level. California was the first state to pass a cyber stalking law, leading to numerous high-profile court cases on the issue since 1999 (Broadhurst & Grabosky, 2005, p. 15).

The VAWA of 1994 is a landmark piece of legislation in the United States aimed at combating various forms of violence against women, including domestic violence, sexual assault, and stalking. One important aspect of VAWA is its recognition of cyberstalking as a form of violence against women. This recognition was a significant step forward in acknowledging the effects of online harassment and stalking on victims' lives.

Despite the inclusion of provisions addressing cyberstalking in VAWA, federal laws, specifically those targeting stalking through electronic means, are relatively limited. This gap in federal legislation has led to a patchwork of laws at the state level, where most cyberstalking legislations are enacted. States have varying definitions and penalties for cyberstalking, creating challenges for law enforcement and prosecutors in effectively addressing these cases (Broadhurst & Grabosky, 2005, p. 18).

California's pioneering role in passing a cyberstalking law in 1999 was a response to the increasing prevalence of online harassment and stalking incidents. This law has been instrumental in prosecuting individuals who engage in cyberstalking, leading to several high-profile court cases that have helped shape the legal landscape around cyberstalking in the United States.

Broadhurst and Grabosky's work provides valuable insights into the evolution of cyberstalking laws and their impact on the judicial system. Their research highlights the importance of addressing cyberstalking through comprehensive legal frameworks that balance the protection of victims' rights with the need to uphold freedom of expression and privacy online.

Overall, the inclusion of cyberstalking provisions in VAWA and the subsequent enactment of state laws demonstrate a growing recognition of the seriousness of online harassment and stalking. However, continued efforts are needed to strengthen federal laws and enhance cooperation between states to effectively combat cyberstalking and ensure justice for victims.

THE SECOND TOPIC:

Hacking

Hacking refers to any attempt to manipulate the natural operations of network connections and linked networks within computer networking. However, the term "hacking" and its practitioners, known as hackers, are now primarily associated with malicious code attacks on the Internet and other networks (Erickson, 2008, p. 06); initially, these "hacks" were considered harmless scientific experiments and educational endeavors, starting in model train clubs and later moving to mainframe computer rooms. With the rise of computer networking and the Internet, data networks became the primary target of malware and hacking activities.

The first requirement: types of Hacking

There are three primary types of hacking based on the hackers' motives and the legality of their actions (Kumar & Agarwal, 2018, p. 245):

I. White Hat Hacking: Also known as ethical hacking, white hat hacking is used for positive purposes. Unlike the stereotypical renegade geniuses depicted in movies, white hat hackers are often employed by large corporations to help enhance their security by identifying vulnerabilities in their systems. Ethical hackers employ many of the same techniques as malicious hackers, but they do so with the permission of the system's owner; ethical hacking is taught in various courses and workshops. (Froehlich, 2023, p. 04).

II. Black Hat Hacking: In contrast to white hat hacking, black hat hacking is often considered unethical. Black hat hackers are typically driven by personal or financial gain although other motives are possible. They exploit phishing emails and compromised websites to access files without the owner's consent. They also use these methods to install malicious software on potential victims' computers to steal their personal information. (Hanna, 2024, p. 24).

III. Gray Hat Hacking: Gray hat hacking falls somewhere between legal and unethical behavior. While gray hat hackers are not necessarily malicious, some of their actions may be perceived as such. For example, they may gain unauthorized access to a network to identify vulnerabilities; they usually inform the owner afterward and request a small fee to fix the issue. If the owner refuses, hackers may publicly disclose their findings, potentially enabling malicious actors to exploit the vulnerabilities. (Tidmarsh, 2023, p. 21).

The second requirement: common Hacking Techniques

Hackers utilize various tools to carry out their attacks, including cross-site scripting, phishing email campaigns, monitoring, and coordinated botnet operations.

Hackers use a variety of tools and techniques to carry out their attacks, each with its own methodology and purpose.

- Cross-Site Scripting (XSS);
- Phishing Email Campaigns;
- Monitoring;
- Coordinated Botnet Operations.

These techniques are constantly evolving as hackers find new ways to exploit vulnerabilities in systems and networks. As such, it is crucial for individuals and organizations to stay vigilant and employ robust security measures to protect against these threats.

I. Phishing

The email instructs the recipient to visit a website where they are prompted to update personal information, such as passwords, credit card details, social security numbers, and bank account numbers, which the legitimate organization have already possessed. In 2003, a phishing scam spread widely, wherein users received emails purportedly from eBay, informing them that their accounts would be suspended unless they clicked on the provided link and updated their credit card information, which eBay already had on record.

Creating a website that resembles a legitimate organization's site is relatively simple by mimicking the HTML code. The scam relied on deceiving people into believing they were being contacted by eBay and subsequently visiting eBay's site to update their account information (Gupta & Anand, 2017, p. 210).

II. Cross-Site Scripting (XSS)

Cross-site scripting (XSS) is a computer security vulnerability commonly found in web applications. It allows malicious web users to inject code into web pages viewed by other users. The XSS attacks involve injecting malicious scripts into trusted websites, causing the browser to execute the script.

Attackers can use XSS to send a malicious script to an unsuspecting user, exploiting vulnerabilities in web applications. There are three main categories of

XSS attacks, mainly reflected, stored, and DOM-based (Shalini &Usha, 2011, p.651).

III. Vishing

Vishing, short for "voice phishing," is a type of electronic fraud that targets individuals over the phone. It is similar to phishing, but instead of using email or text messages, vishing attacks use voice technology to deceive victims into revealing sensitive information, such as credit card numbers, social security numbers, or passwords. Unlike phishing, vishing does not always occur over the Internet but instead uses voice technologies such as voice email, VoIP, traditional landline, or cellular phones.

Tracking vishing attacks is challenging for authorities, especially when VoIP is used. Additionally, vishing scams are often outsourced to other countries, making it difficult for law enforcement to intervene (Yeboah-Boateng & Amanor, 2014, p. 300).

IV. Bot Networks

Bot networks, a form of cybercrime, are increasingly prevailing. In this type of attack, spammers and cybercriminals remotely take control of computers without the users' knowledge. Users unknowingly download malware such as Trojan horses, which then connect their computers to bot networks. These compromised machines, or "zombies," can be triggered to work together, providing attackers access to the processing power of thousands of computers. Attackers often use bot networks to speed up and expand their attacks by scanning for vulnerable systems. The use of bot networks is considered one of the most significant developments in cybercrime (Broadhurst &Grabosky, 2005, p. 17).

THE THIRD TOPIC:

Cybercrime Examples

This section explores prominent instances of various cybercrime attacks employed by cybercriminals. Cybercriminals use a variety of tactics to commit cybercrimes, including phishing, malware attacks, ransomware, and denial-of-service (DoS) attacks. These attacks are often designed to steal sensitive information, such as passwords or financial data, disrupt services, or extort money from victims. Understanding these tactics is crucial for developing effective cybersecurity strategies.

The first requirement: navigating the landscape of cybercrime: malware and phishing attacks

I. Malware Attacks

A malware attack involves infecting a computer system or network with malicious software, such as computer viruses or other types of malwares. Cybercriminals can use a compromised computer for various purposes. Malware attacks can target all kinds of devices and operating systems, including Microsoft Windows, macOS, Android, and iOS (Gupta, 2013, pp. 5-7).

One well-known example of a malware attack is the WannaCry ransomware attack; a global cybercrime that occurred in May 2017. Ransomware is a type of malware used to extort money by encrypting the victim's data or device and demanding payment.

II. Phishing and Social Engineering Attacks

Phishing involves sending deceptive messages to internet users, typically via email, to trick them into divulging personal information, visiting malicious websites, or downloading malicious software.

In 2018, a phishing scam during the World Cup targeted football fans with emails containing infected attachments or links to malicious sites. Another type of phishing campaign, known as spear-phishing, targets specific individuals within an organization to compromise its security. An example of a large-scale data breach due to phishing is Yahoo's data leak between 2013 and 2016, which exposed three billion user accounts (McAndrew, 2021, p. 02).

In 2023, cybercriminals continued to exploit phishing tactics to target individuals and organizations. One notable incident involved a phishing campaign that impersonated popular social media platforms, tricking users into clicking on malicious links and compromising their accounts. Another phishing attack targeted employees of a major corporation, using sophisticated tactics to gain access to sensitive company information. These incidents highlight the ongoing threat posed by phishing attacks and the importance of vigilance in recognizing and responding to suspicious emails and messages.

The second requirement: distributed denial-of-service (DDoS) attacks

The DDoS attacks involve using multiple connected Internet of Things (IoT) devices to overwhelm a target's network, making it inaccessible to legitimate users. Cybercriminals may use DDoS attacks as a distraction tactic or to extort money.

In 2016, the largest-ever DDoS attack occurred, affecting over 1 million IoT devices that were hacked due to technical vulnerabilities. This attack disrupted the global Domain Name System (DNS) and popular websites like Twitter, Netflix, and PayPal (Mahjabin, et al, 2017, p. 2).

In 2023, the threat of DDoS attacks persisted, with cybercriminals targeting IoT devices to launch large-scale attacks. One significant incident involved a DDoS attack that disrupted critical services and popular websites, including social media platforms, streaming services, and online payment platforms. This attack highlighted the vulnerability of IoT devices and the need for enhanced security measures to protect against such threats.

THE FOURTH TOPIC:

The future of cybercrime

The future of cybercrime is a topic of an increasing concern as technology advances and cybercriminals become more sophisticated. Predicting the future of cybercrime involves understanding current trends and anticipating how they might evolve. This includes the development of new cyber threats, such as artificial intelligence-powered attacks and the use of emerging technologies like quantum computing to bypass traditional security measures. Addressing the future of cybercrime requires ongoing innovation in cybersecurity practices and technologies to stay ahead of cybercriminals.

The first requirement: safeguarding tomorrow: a comprehensive approach to cybercrime prevention

Reducing cybercrime requires a multifaceted approach that includes aligning with legislation, laws, protocols, best practices, and policies. By implementing a cybercrime system, organizations and companies can better protect their networks and technologies. Public-private partnership outreach programs can also help understand the impact of new technologies on cybercrime and conduct research to address future threats. While cybercriminals constantly evolve, closing the gap requires creative enforcement of cybercrime detection, research, prosecutions, and compliance initiatives, along with staying current on laws and best practices.

A Juniper Research report predicts that data breach costs will reach five trillion dollars by 2024, driven in part by fines from data privacy laws like the General Data Protection Regulation (GDPR) and the California Consumer Privacy

Act. Artificial intelligence is expected to play a significant role in this increase, as both companies and threat actors leverage AI for cyberattacks (www.infosecurity-magazine.com, 2019, p 05).

The second requirement: how to protect yourself against cybercrime

Protecting yourself against cybercrime is essential in today's digital world; this involves implementing strong cybersecurity practices to safeguard your personal information and devices from malicious actors. By using strong and unique passwords, enabling two-factor authentication, keeping your software up to date, and being cautious of phishing attempts, you can significantly reduce the risk of falling victim to cybercrime. Additionally, being mindful of the information you share online and regularly backing up your data can further enhance your cybersecurity posture. After explaining the risks and forms of cybercrime, it is essential to understand how to safeguard our devices and personal information effectively.

1. Maintain an up-to-date operating system and software: Regularly update your applications and operating system to ensure you have the latest security patches and protections (1stsecuritybank.com).

2. Use anti-virus software and keep it updated: Utilize anti-virus software to scan for, detect, and remove threats. Ensure your software is regularly updated for optimal protection.

3. Use strong passwords: Create strong, unique passwords and avoid recording them in insecure locations (Parker, 2020, p 12).

4. Never open attachments in spam emails: Avoid opening attachments from unknown senders to prevent malware infections.

5. Do not click on links in spam emails or untrusted websites: Clicking on links in spam emails or unfamiliar websites can lead to cybercrime. Be cautious and avoid clicking on suspicious links (araglegal.com).

6. Do not give out personal information unless secure: Refrain from sharing personal information over the phone or email unless you are certain of the recipient's identity and security measures.

7. Contact companies directly about suspicious requests: If you receive a suspicious request for data, verify its legitimacy by contacting the company directly using the contact information on their official website.

8. Be mindful of website URLs: Ensure the websites you visit have secure URLs (https) and consider using internet security features for online transactions.

9. Monitor your bank statements: Regularly check your bank statements for any unauthorized transactions and report them to your bank promptly.

Conclusion:

The escalating complexity of cyber threats poses significant challenges to securing our digital world. As technology advances and internet connectivity becomes ubiquitous, the risk of cybercrime continues to grow. Accordingly, it is essential for individuals, organizations, and governments to remain vigilant and proactive in combating cyber threats.

This research has shed light on the diverse forms of cybercrime and their far-reaching consequences. By understanding these risks and adopting best practices, such as maintaining up-to-date security measures and fostering a culture of cyber awareness, one can mitigate the impact of cyber-attacks.

Looking ahead, it is crucial to prioritize cybersecurity through flexible legislation, robust institutional frameworks, and ongoing education. By investing in innovative solutions and fostering collaboration across sectors, individuals can enhance their resilience against cyber threats and protect their digital future.

Recommendations and suggestions

1. Enhance Legislative and Institutional Flexibility: Continuously review and update laws and regulations to address evolving cyber threats. Provide flexibility in frameworks to adapt to new technologies and cybercrime tactics.

2. Invest in Anti-Cybercrime Capacity Building: Develop comprehensive training programs and resources for individuals, organizations, and law enforcement agencies to enhance their capabilities in detecting, preventing, and responding to cyber threats.

3. Support Innovation in Anti-Cybercrime Technologies: Invest in research and development of new technologies and tools to combat cybercrime effectively. Encourage collaboration between industry, academia, and government to drive innovation in cybersecurity.

4. Strengthen Regulatory Environment: Establish clear guidelines and regulations for cybersecurity practices in various sectors. Ensure that regulatory frameworks are adaptable to emerging threats and technologies.

5. Enhance Cybersecurity Awareness and Education: Educate individuals and organizations about the importance of cybersecurity and best practices for protecting against cyber threats. Provide training and resources to build cyber resilience.

6. Foster Public-Private Partnerships: Establish collaborative efforts between government, industry, and academia to share information and resources for combating cyber threats. This can improve coordination and response capabilities.

7. Implement Cybersecurity Risk Management: Develop and implement cybersecurity risk management strategies that prioritize critical assets and vulnerabilities. This can help organizations better allocate resources and respond to cyber threats effectively.

8. Enhance International Cooperation: Strengthen cooperation and information sharing on cyber threats and best practices at the international level. This can help create a unified front against cybercrime and cyber threats.

9. Encourage Adoption of Cybersecurity Standards: Promote the adoption of cybersecurity standards and best practices, such as ISO 27001, NIST Cybersecurity Framework, and others to ensure a consistent and effective approach to cybersecurity across industries.

Establish Incident Response Plans: Develop and implement incident response plans that outline steps to take in the event of a cyber-attack. Regularly test and update these plans to ensure they are effective.

References:

1. Boateng, Y., & Amanor, P. M. (2014, April). *Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices*. *Journal of Emerging Trends in Computing and Information Sciences*, 5(4). ISSN 2079-8407.
2. Bocij, P. (2004). *Cyber Stalking - Harassment in the Internet age and How to protect your family*. Library of Congress Cataloging-in-Publication Data, ISBN:0-275-98118-5.
3. Broadhurst R., & Grabosky, P. (2005). *Cyber Crime – The Challenges in Asia*. Hong Kong University Press. ISBN: 962-209-724-3.
4. Erickson, J. (2008). *Hacking – The Art of Exploitation (2nd Ed.)*. William Pollock Publishers. ISBN: 1-59327-144-1.
5. Froehlich, A. (2024, Nov. 23). Retrieved from <http://www.techtarget.com/searchsecurity/definition/cybersecurity-asset-management-CSAM>.
6. Gupta, A., & Anand, A. (2017, April). *Ethical Hacking and Hacking Attacks*. *International Journal of Engineering and Computer Science*, 6 (4), 21042-21050. ISSN: 2319-7242.
7. Gupta, S. (2013, January). *Types of Malware and its Analysis*. *International Journal of Scientific & Engineering Research*, 4(1). ISSN 2229-5518.
8. Hanna, K. T. (2024, Feb. 09). Retrieved from <http://www.techtarget.com/searchsecurity/definition/cyberterrorism>.
9. Kumar, S., Agarwal, D. (2018, April). *Hacking Attacks, Methods, Techniques And Their Protection Measures*. *IJSART*, 4(4). ISSN (Online): 2395-1052.
10. Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). *A survey of distributed denial-of-service attack, prevention, and mitigation techniques*. *International Journal of Distributed Sensor Networks*, 13(12). ISSN: 1550-1477.
11. McAndrew, E. J. (2018). *The Hacked & the Hacker-for-Hire: Lessons from the Yahoo Data Breaches (So Far)*. *The National Law Review*, XI(106), 2161 – 3362.
12. Parker, T. (2020, Feb.). Retrieved from <http://www.investopedia /financial-edge/0712/6-ways-to-protect-yourself-against-cybercrime.aspx>.
13. Pittaro, M. (). – *Cyber stalking: An Analysis of Online Harassment and Intimidation*, *International Journal of Cyber Criminology (IJCC)*, 1(2), 180–197. ISSN: 0974 – 2891.
14. Shalini1, S., & Usha, S. (2011, July). *Prevention Of Cross-Site Scripting Attacks (XSS) On Web Applications In The Client Side*. *International Journal of Computer Science Issues*, 8(4). ISSN (Online): 1694-0814.
15. Tidmarsh, D. (2023, Nov. 7). Retrieved from <http://www.eccouncil.org /cybersecurity-exchange/ethical-hacking>.
16. <https://www.towergateinsurance.co.uk/hub/care-medical/how-to-protect-yourself-against-cybercrime>.
17. https://www.1stsecuritybank.com/about/blog/blog_details/?news_cat=blog&news_article=5_ways_to_protect_yourself_from_cybercrime.
18. www.araglegal.com/individuals/learning-center/topics/protecting-your-identity/cyber-crime-prevention.
19. www.infosecurity-magazine.com /news/breach-costs-trillion.

