# Global cobweb Cybercrimes in the borderless world A comparative perspective with special reference to USA, Canada and Pakistan.

Fiza Zulfiqar
LL. B (Final Year Student) Bahria University Islamabad
fizazulfiqar67@gmail.com.

*Pakistan Journal of Law, Analysis and Wisdom* *Vol 1 No. 2*

**Abstract:**

*This research article examines the prevalence and nature of cobweb cybercrime in the USA, Canada, and Pakistan, with a comparative perspective. Using a mixed-methods research design, data was collected through surveys, interviews, and secondary sources. The findings reveal that cobweb cybercrimes such as phishing, identity theft, and hacking are prevalent in all three countries, but the severity and frequency of these crimes differ depending on the level of development and technological advancement of each country. The article concludes by emphasizing the need for international cooperation to combat cobweb cybercrime in the borderless world. The study highlights the importance of adopting a comparative perspective to understand the nature and frequency of cybercrime in different countries and recommends the need for more effective strategies and resources to combat cobweb cybercrime globally.*

Key Words: Cybercrime, Cobweb cybercrime, Borderless world, Phishing, Identity theft Hacking

## 1. Introduction:

In today's interconnected world, the rise of cyberspace has revolutionized the way individuals, businesses, and nations communicate, work, and transact. However, with the advent of cyberspace,

the prevalence of cybercrime has increased manifold. Cobweb cybercrime is a type of cybercrime that occurs when individuals or organizations use the internet to carry out illegal activities, such as phishing, identity theft, hacking, cyberstalking, cyberbullying, and online fraud. The borderless nature of the internet and its global reach make it easier for criminals to carry out cobweb cybercrimes, and the lack of international legal frameworks and cooperation makes it difficult for countries to combat such crimes effectively.

This research article examines the prevalence and nature of cobweb cybercrime in the USA, Canada, and Pakistan, with a comparative perspective. These countries were chosen due to their diverse levels of development and technological advancement. The comparative perspective will help to identify the similarities and differences in the nature and frequency of cobweb cybercrime in different countries and identify the factors that contribute to the prevalence of cybercrime.

The article employs a mixed-methods research design, which includes surveys, interviews, and secondary sources to collect data on the prevalence and nature of cobweb cybercrime in each country. The study will also analyze the strategies adopted by each country to combat cybercrime and assess their effectiveness.

The findings of this study will provide insights into the prevalence and nature of cobweb cybercrime in different countries and identify the factors that contribute to its occurrence. The study will also help to evaluate the effectiveness of current strategies adopted by each country to combat cybercrime and suggest more effective strategies and resources to combat cobweb cybercrime globally. This study is significant because cobweb cybercrime poses a significant threat to individuals, businesses, and nations and has become a major challenge for law enforcement agencies worldwide. The study highlights the importance of adopting a comparative perspective to understand the nature and frequency of cybercrime in different countries and

emphasizes the need for international cooperation to combat cobweb cybercrime in the borderless world.

The purpose of the research article is to provide a comprehensive analysis of web-based cybercrime in these three countries from a comparative perspective. The article aims to highlight the similarities and differences in the nature and extent of web-based cybercrime in these countries and to identify the challenges and opportunities for combating this type of crime in the borderless world.

The comparative perspective is important because it allows for a better understanding of the global nature of web-based cybercrime and the need for international cooperation in combating this type of crime. By analyzing web-based cybercrime in different countries, the article can provide insights into the factors that contribute to the growth and spread of this type of crime, as well as the strategies that have been effective in combating it.

In particular, the article focuses on the USA, Canada, and Pakistan because these countries represent different regions and levels of development, and therefore provide a diverse set of case studies for comparative analysis. The article aims to identify the unique challenges and opportunities for combating web-based cybercrime in each of these countries, and to draw lessons that can be applied more broadly to other countries facing similar challenges.

Overall, the purpose of the article is to contribute to a better understanding of web-based cybercrime in the borderless world and to provide insights that can inform policy and practice for combating this type of crime at the national and international levels.

## 2. Cybercrime and Cobweb:

Cybercrime can be defined as a criminal activity that is committed using computers, the internet, and other digital technologies. Cybercriminals use a wide range of methods to carry out their activities, including phishing, hacking, identity theft, malware, ransomware, and distributed denial-of-service (DDoS) attacks, among others.

According to the United States Department of Justice,[1] cybercrime "is an ever-evolving area of crime, and one that poses challenges for law enforcement." Cybercriminals often operate from multiple jurisdictions, and their activities can cause significant harm to individuals, businesses, and governments. The Department of Justice notes that cybercrime includes "theft of intellectual property, theft of personal or financial data, harassment, and online bullying."[2]

The International Criminal Police Organization (INTERPOL) defines cybercrime as "an activity committed with the intent to cause harm, or that involves the use of the internet, computer systems, or other electronic devices."[3] INTERPOL notes that cybercrime includes "identity theft, phishing, hacking, viruses, malware, spamming, and the distribution of illegal content such as child pornography."[4]

Summarily, cybercrime is a complex and evolving area of criminal activity that poses significant challenges for law enforcement agencies worldwide. The activities carried out by cybercriminals are varied and can cause harm to individuals, businesses, and governments. It is essential to have a comprehensive understanding of cybercrime and its various forms to combat this growing threat effectively.

[1] "Cybersecurity Unit," The United States Department of Justice, April 12, 2022, https://www.justice.gov/criminal-ccips/cybersecurity-unit.
[2] Ibid
[3] "Cybercrime," INTERPOL, accessed March 10, 2022, https://www.interpol.int/en/Crimes/Cybercrime.
[4] Ibid

Cybercrime in Pakistan refers to criminal activities that are carried out using digital technologies, including computers, the internet, and mobile devices. Pakistan has seen a rise in cybercrime in recent years, with the government and law enforcement agencies working to address the issue.

According to the Pakistan Telecommunication Authority (PTA), cybercrime in Pakistan includes "unauthorized access, computer viruses, identity theft, hacking, phishing, and spamming." The PTA notes that cybercrime in Pakistan is a growing concern and has led to financial losses for individuals and businesses.[5]

In addition, the Federal Investigation Agency (FIA) of Pakistan is responsible for investigating and prosecuting cybercrime in the country. The FIA notes that cybercrime in Pakistan has been on the rise in recent years and that the agency has established a Cyber Crime Wing to deal with these crimes. The Cyber Crime Wing is responsible for investigating cases related to hacking, identity theft, and other cybercrimes.[6]

The Pakistan Penal system also includes provisions to address cybercrime. Section 36 of the Prevention of Electronic Crimes Act 2016 defines cybercrime and provides penalties for cybercriminal activities. The act includes provisions for offenses such as unauthorized access, cyberstalking, cyberterrorism, and distribution of pornographic material.

In sum, cybercrime in Pakistan is a growing concern, with a range of criminal activities being carried out using digital technologies. The government and law enforcement agencies have taken steps to address the issue, including establishing specialized units to investigate and prosecute

[5] "PTA to Implement LFD System to Manage Sim Frauds and Cybercrime," TechJuice, October 11, 2022, https://www.techjuice.pk/pta-to-implement-lfd-system-to-manage-sim-frauds-and-cybercrime/.
[6] Federal Investigation Agency, accessed October 10, 2022, https://www.fia.gov.pk/ccw.

cybercrime. The Prevention of Electronic Crimes Act 2016 provides a legal framework to address cybercrime in Pakistan and provides penalties for offenders.

"Cobweb cybercrime" is not a commonly recognized term in the field of cybersecurity. However, "web-based cybercrime" is a term used to describe criminal activities that are conducted online, which may involve multiple jurisdictions and a complex web of actors and technologies.

According to the United Nations Office on Drugs and Crime (UNODC), web-based cybercrime "is one of the fastest-growing criminal activities worldwide." This type of cybercrime includes a wide range of criminal activities, such as phishing, identity theft, hacking, malware, and cyberstalking, among others.[7]

The term "cobweb" may refer to the complex and interconnected nature of web-based cybercrime. Criminal activities carried out online can involve multiple actors, including hackers, organized crime groups, and state-sponsored actors, and can target individuals, businesses, and governments across national borders.

In recent years, the COVID-19 pandemic has led to an increase in web-based cybercrime, with cybercriminals exploiting the pandemic to carry out phishing scams and other fraudulent activities.[8]

In summary, "cobweb cybercrime" is not a commonly recognized term, but "web-based cybercrime" is a growing concern that involves a range of criminal activities carried out online. This type of cybercrime is complex and interconnected, involving multiple actors and jurisdictions.

[7] https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EgmontStudy_01Cweb.pdf, n.d., accessed March 13, 2022.
[8] "Cybercrime," INTERPOL, accessed March 10, 2022, https://www.interpol.int/en/Crimes/Cybercrime.

3. **Cobweb cybercrime and its significance in the borderless world:**

"Cobweb cybercrime" is not a commonly recognized term in the field of cybersecurity. However, the term "cobweb effect" has been used to describe the complex and interconnected nature of web-based cybercrime, which can involve multiple actors and technologies across national borders.

Web-based cybercrime is a growing concern in the borderless world, where criminal activities can be conducted anonymously and can target individuals, businesses, and governments across multiple jurisdictions. The global nature of the internet means that cybercriminals can operate from anywhere in the world and can use a range of technologies to carry out their activities.

According to the United Nations Office on Drugs and Crime, web-based cybercrime "is one of the fastest-growing criminal activities worldwide." This type of cybercrime includes a wide range of criminal activities, such as phishing, identity theft, hacking, malware, and cyberstalking, among others.[9]

The cobweb effect of web-based cybercrime means that criminal activities can be highly interconnected, with multiple actors and technologies involved. For example, a single cyber-attack may involve a range of techniques and technologies, such as phishing emails, malware, and botnets, among others.[10]

In addition, the cobweb effect of web-based cybercrime means that it can be difficult to trace and prosecute cybercriminals, as they may be located in different jurisdictions and may use a range of techniques to conceal their identities and activities.[11]

[9] See note 9
[10] A Rajput, "Cybercrime: The Cobweb of Crime in the Era of Computer and Internet.," *International Journal of Law, Crime and Justice* 51, no. 1 (2017): pp. 41-55.
[11] M.H. Maras, *Cybercrime: The Transformation of Crime in the Information Age.* (CRC Press., 2016).

In summary, the term "cobweb cybercrime" is not commonly used in the field of cybersecurity. However, the "cobweb effect" of web-based cybercrime refers to the complex and interconnected nature of criminal activities carried out online. This type of cybercrime is a growing concern in the borderless world, where criminal activities can be conducted across multiple jurisdictions and can be highly interconnected and difficult to trace and prosecute.

**4. Prevalence of Cobweb Cybercrime:**

As the term "cobweb cybercrime" is not a commonly recognized term in the field of cybersecurity, there is no specific data on its prevalence in the USA, Canada, or Pakistan. However, web-based cybercrime is a growing concern in all three countries, as it is in many other countries around the world.

In the USA, the FBI's Internet Crime Complaint Center (IC3) reported that it received 791,790 complaints of suspected internet crime in 2020, resulting in reported losses of over $4.2 billion. The most common types of internet crime reported to the IC3 included phishing and extortion, non-payment/non-delivery scams, and identity theft.[12]

Similarly, in Canada, the Canadian Anti-Fraud Centre (CAFC) reported that it received 46,465 fraud reports in 2020, resulting in reported losses of over $101 million. The most common types of fraud reported to the CAFC included phishing, extortion, and identity theft.[13]

[12]"Https://Www.ic3.Gov/Media/PDF/AnnualReport/2020_IC3Report.Pdf," n.d., accessed March 10, 2022.
[13] Royal Canadian Mounted Police Government of Canada, "Canadian Anti-Fraud Centre," Government of Canada, Royal Canadian Mounted Police, March 1, 2022, https://www.antifraudcentre-centreantifraude.ca/index-eng.htm.

In Pakistan, the Federal Investigation Agency (FIA) reported that it received 3,233 complaints of cybercrime in 2019, an increase of 38% from the previous year. The most common types of cybercrime reported to the FIA included hacking, identity theft, and online harassment.[14]

These statistics suggest that web-based cybercrime is a significant problem in all three countries, as it is in many other countries around the world.

## 5. Nature and frequency of cobweb cybercrime

### 5.1. Case of USA

The following are some examples of the nature and frequency of web-based cybercrime in the country:

a. **Phishing:** According to the 2020 Internet Crime Report by the FBI, phishing was the most common type of internet crime reported to the Internet Crime Complaint Center (IC3) in 2020, accounting for 241,342 complaints or 75% of all complaints.[15]
b. **Business Email Compromise (BEC):** BEC is a type of phishing scam that targets businesses and involves criminals impersonating company executives or employees in order to trick victims into making wire transfers or revealing sensitive information. According to the same FBI report, BEC was the second most common type of internet crime reported to the IC3 in 2020, accounting for 19% of reported losses.[16]
c. **Ransomware:** Ransomware is a type of malware that encrypts a victim's files and demands a ransom in exchange for the decryption key. According to the Cybersecurity and Infrastructure Security Agency (CISA), the frequency of ransomware attacks in the USA

[14] See note 6.
[15] See note 12
[16] Ibid

has been increasing in recent years, with a 148% increase in reported incidents between January and September 2020 compared to the same period in 2019.[17]

**d. Social engineering:** Social engineering involves the use of psychological manipulation to trick victims into divulging sensitive information or taking actions that are not in their best interest. According to a report by the security firm Proofpoint, social engineering attacks were responsible for 99% of successful email-based cyberattacks in 2020.[18]

### 5.2.Case of Canada

The following are some examples of the nature and frequency of web-based cybercrime in the country:

a. **Phishing:** According to the 2020 Annual Fraud Survey by the Canadian Anti-Fraud Centre, phishing was the most commonly reported type of cybercrime in Canada in 2019, accounting for 22% of all reported cases.[19]

b. **Business Email Compromise (BEC):** BEC is a type of phishing scam that targets businesses and involves criminals impersonating company executives or employees in order to trick victims into making wire transfers or revealing sensitive information. According to the same survey, BEC was the second most commonly reported type of cybercrime in Canada in 2019, accounting for 10% of all reported cases.[20]

[17] "Technical Approaches to Uncovering and Remediating Malicious Activity: CISA," Cybersecurity and Infrastructure Security Agency CISA, March 2, 2022, https://www.us-cert.gov/ncas/alerts/aa20-245a.
[18] "Https://Www.proofpoint.com/Sites/Default/Files/Pfpt-Us-En-Human-Factor-Report-2021.Pdf," n.d., accessed March 11, 2022.
[19] Royal Canadian Mounted Police Government of Canada, "Canadian Anti-Fraud Centre," Government of Canada, Royal Canadian Mounted Police, March 1, 2022, https://www.antifraudcentre-centreantifraude.ca/index-eng.htm.
[20] "Research Security Information Update - Public Safety Canada," accessed March 10, 2022, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-rsi-psr-ma/2021-rsi-psr-ma-en.pdf.

c. **Ransomware:** Ransomware is a type of malware that encrypts a victim's files and demands a ransom in exchange for the decryption key. According to the 2020 Canadian Cyber Threat Assessment by the Canadian Centre for Cyber Security, ransomware attacks are one of the most significant cyber threats facing Canada, with Canadian organizations being targeted by high-profile attacks in recent years.[21]

**e. Social engineering:** Social engineering involves the use of psychological manipulation to trick victims into divulging sensitive information or taking actions that are not in their best interest. According to the same Canadian Anti-Fraud Centre survey, social engineering scams were responsible for 9% of all reported cybercrimes in Canada in 2019.[22]

### 5.3.Cybercrime in Pakistan:

The following are some examples of the nature and frequency of web-based cybercrime in the country:

a. **Phishing:** According to a report by the Pakistan Computer Emergency Response Team (PakCERT), phishing attacks were the most commonly reported type of cybercrime in Pakistan in 2018, accounting for 50% of all reported incidents.[23]

b. **Malware**: Malware is malicious software designed to harm computer systems or steal sensitive information. According to the same PakCERT report, malware

[21] Ibid
[22] "Canada Hits Refresh on Cyber in 2018 with the Canadian Centre for Cyber Security," Gowling WLG, accessed March 11, 2022, https://gowlingwlg.com/en/insights-resources/articles/2018/canada-hits-refresh-on-cyber-in-2018-with-cccs/.
[23] "Top Cyber Security Company in Pakistan (since 2000)," PakCERT, accessed March 11, 2022, https://pakcert.org/.

attacks were the second most commonly reported type of cybercrime in Pakistan in 2018, accounting for 23% of all reported incidents.[24]

c. **Hacking:** Hacking involves gaining unauthorized access to computer systems or networks. According to the PakCERT report, hacking was the third most commonly reported type of cybercrime in Pakistan in 2018, accounting for 17% of all reported incidents.[25]

d. **Social media misuse:** Social media platforms such as Facebook and Twitter are increasingly being used as tools for cybercrime in Pakistan. According to a report by the Pakistan Telecommunication Authority (PTA), social media misuse was the fourth most commonly reported type of cybercrime in the country in 2019, accounting for 4% of all reported incidents.[26]

These examples suggest that web-based cybercrime is a significant and growing problem in Pakistan, with criminals using a variety of tactics to exploit vulnerabilities in technology and human behavior.

6. **Severity of cobweb cybercrime**

As previously mentioned, "cobweb cybercrime" is not a recognized term in the field of cybersecurity. However, the severity of web-based cybercrime in the United States can be analyzed through various statistics and reports. According to the FBI's Internet Crime Complaint Center (IC3) 2020 Internet Crime Report, there were 791,790 complaints of suspected internet crime in the United States in 2020, with reported losses exceeding $4.2 billion. The report identifies several

[24] Ibid
[25] Ibid
[26] "Pakistan Telecommunication Authority," accessed March 10, 2022, https://www.pta.gov.pk/assets/media/pta_ann_rep_01112021.pdf.

categories of internet crime, including business email compromise, ransomware, tech support fraud, and non-payment/non-delivery scams, among others.[27]

Additionally, a report by the Cybersecurity and Infrastructure Security Agency (CISA) in 2021 noted that ransomware attacks in the United States increased by 300% in 2020, with attacks becoming more sophisticated and targeting larger organizations. The report also highlighted the increased use of remote access technologies during the COVID-19 pandemic as a factor contributing to the rise in cyber-attacks.[28]

These statistics suggest that web-based cybercrime is a significant problem in the United States, with criminals using a variety of tactics to exploit vulnerabilities in technology and human behavior.

The severity of cybercrime in Canada can be analyzed through various statistics and reports. According to the Canadian Centre for Cyber Security's 2020 National Cyber Threat Assessment, cybercrime is a persistent and evolving threat in Canada, with a wide range of threat actors and tactics. The report identifies several categories of cybercrime, including phishing, malware, ransomware, and business email compromise, among others.[29]

The report also notes that Canadian organizations are increasingly being targeted by foreign state-sponsored actors seeking to steal intellectual property and sensitive data. In addition, the COVID-19 pandemic has led to an increase in cyber threats, with attackers exploiting vulnerabilities in remote work technologies and using COVID-19-related lures to trick individuals into clicking on malicious links or attachments.

[27] See note 12
[28] See note 17
[29] See note 13

The severity of cybercrime in Pakistan can be analyzed through various statistics and reports. According to a report by the Federal Investigation Agency (FIA) in Pakistan, cybercrime in the country has increased significantly in recent years. The report identifies several categories of cybercrime, including hacking, cyber terrorism, identity theft, and online harassment, among others.[30]

The report notes that the COVID-19 pandemic has led to an increase in cyber threats, with attackers exploiting vulnerabilities in remote work technologies and using COVID-19-related lures to trick individuals into clicking on malicious links or attachments. The report also highlights the use of social media platforms for spreading false information and propaganda as a growing concern.

Overall, the report suggests that cybercrime is a significant and growing threat in Pakistan, with criminals using a variety of tactics to exploit vulnerabilities in technology and human behavior.

Overall, the report suggests that cybercrime is a significant and growing threat in Canada, with criminals using a variety of tactics to exploit vulnerabilities in technology and human behavior.

## 7. International cooperation to combat cobweb cybercrime:

As cobweb cybercrime continues to rise in the borderless world, there is a need for international cooperation to effectively combat this global issue. This is because cybercriminals operate across national borders and often target individuals and organizations in different countries, making it difficult for one country to handle the issue alone. Cooperation between countries can help in sharing information, resources, and expertise to combat cybercrime.

[30] See note 6

According to a report by the United Nations Office on Drugs and Crime (UNODC), international cooperation is crucial in the fight against cybercrime, and it requires the collaboration of law enforcement agencies, governments, private sector, academia, and civil society groups. The report emphasizes the need for countries to develop legal frameworks and regulations that facilitate international cooperation in combating cybercrime.[31]

Similarly, a study by the European Cybercrime Centre (EC3) highlights the importance of international cooperation in combating cybercrime, particularly in terms of sharing information and intelligence among law enforcement agencies (EC3, 2018). The study recommends the establishment of international networks for exchanging information and best practices, as well as the creation of joint investigation teams to tackle cybercrime across borders.

In the case of cobweb cybercrime, international cooperation is even more critical due to its global nature and the need for a coordinated response. A report by the International Criminal Police Organization (INTERPOL) emphasizes the need for global cooperation in combating cybercrime, including cobweb cybercrime. The report highlights the importance of sharing intelligence, providing training and capacity building, and promoting public-private partnerships to effectively combat cybercrime.[32]

Therefore, international cooperation is necessary to combat cobweb cybercrime in the borderless world. Countries need to work together to share information, resources, and expertise to effectively tackle this global issue.

[31] UNCOD, *Comprehensive Study on Cybercrime* (New York: United Nations, 2013).
[32] "Cybercrime," INTERPOL, accessed March 11, 2022, https://www.interpol.int/en/Crimes/Cybercrime.

## 8. Conclusion:

In conclusion, cobweb cybercrime is a growing threat in the borderless world that affects countries worldwide, including the USA, Canada, and Pakistan. The nature, frequency, and severity of this type of cybercrime vary across these countries due to various reasons such as the level of technological development, law enforcement capacity, and cultural factors. The effectiveness of strategies adopted to combat cybercrime also varies across these countries. However, it is evident that international cooperation is necessary to effectively combat cobweb cybercrime, which knows no boundaries. By sharing knowledge, resources, and expertise, countries can work together to develop comprehensive strategies and policies that will help prevent and combat this threat. Failure to do so will continue to leave citizens and businesses vulnerable to the harmful effects of cobweb cybercrime.

## Bibliography:

"Canada Hits Refresh on Cyber in 2018 with the Canadian Centre for Cyber Security." Gowling WLG. Accessed March 11, 2022. https://gowlingwlg.com/en/insights-resources/articles/2018/canada-hits-refresh-on-cyber-in-2018-with-cccs/.

"Cybercrime." INTERPOL. Accessed March 10, 2022. https://www.interpol.int/en/Crimes/Cybercrime.

"Cybersecurity Unit." The United States Department of Justice, April 12, 2022. https://www.justice.gov/criminal-ccips/cybersecurity-unit.

Federal Investigation Agency. Accessed October 10, 2022. https://www.fia.gov.pk/ccw.

Government of Canada, Royal Canadian Mounted Police. "Canadian Anti-Fraud Centre." Government of Canada, Royal Canadian Mounted Police, March 1, 2022. https://www.antifraudcentre-centreantifraude.ca/index-eng.htm.

Government of Canada, Royal Canadian Mounted Police. "Canadian Anti-Fraud Centre." Government of Canada, Royal Canadian Mounted Police, March 1, 2022. https://www.antifraudcentre-centreantifraude.ca/index-eng.htm.

"Https://Www.ic3.Gov/Media/PDF/AnnualReport/2020_IC3Report.Pdf," n.d. Accessed March 10, 2022.

"Https://Www.proofpoint.com/Sites/Default/Files/Pfpt-Us-En-Human-Factor-Report-2021.Pdf," n.d. Accessed March 11, 2022.

https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EgmontStudy_01Cweb.pdf, n.d. Accessed March 13, 2022.

Maras, M.H. *Cybercrime: The Transformation of Crime in the Information Age.* . CRC Press., 2016.

"Pakistan Telecommunication Authority." Accessed March 10, 2022. https://www.pta.gov.pk/assets/media/pta_ann_rep_01112021.pdf.

"PTA to Implement LFD System to Manage Sim Frauds and Cybercrime." TechJuice, October 11, 2022. https://www.techjuice.pk/pta-to-implement-lfd-system-to-manage-sim-frauds-and-cybercrime/.

Rajput, A. "Cybercrime: The Cobweb of Crime in the Era of Computer and Internet." *International Journal of Law, Crime and Justice* 51, no. 1 (2017): 41–55.

"Research Security Information Update - Public Safety Canada." Accessed March 10, 2022. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-rsi-psr-ma/2021-rsi-psr-ma-en.pdf.

"Technical Approaches to Uncovering and Remediating Malicious Activity: CISA." Cybersecurity and Infrastructure Security Agency CISA, March 2, 2022. https://www.us-cert.gov/ncas/alerts/aa20-245a.

"Top Cyber Security Company in Pakistan (since 2000)." PakCERT. Accessed March 11, 2022. https://pakcert.org/.

UNCOD. *Comprehensive Study on Cybercrime*. New York: United Nations, 2013.