Packet Sniffing in the Cyber Threat Landscape: Examining Wireshark Capabilities, Misuse, and Policy Options in the Philippines

Adrian B. Silvestre[1] and Julina Rose DL. De Ocampo[2]

[1]Far Eastern University, General Education Department, Manila, Philippines

[2]New Era University, College of Law, Quezon City, Philippines

DOI: https://dx.doi.org/10.47772/IJRISS.2023.7856

Received: 26 July 2023; Revised: 10 August 2023; Accepted: 14 August 2023; Published: 09 September 2023

ABSTRACT

Wireshark is an invaluable network analysis tool, yet its traffic sniffing abilities also introduce privacy and security risks. This study analyzed Wireshark's capabilities, cyber threats enabled through its misuse, and challenges in regulating open-source software. A literature review examined technical details, risks, and legal violations including illegal access, data theft, and denial-of-service attacks. Interviews with law enforcement uncovered constraints in prohibiting publicly accessible tools like Wireshark directly. Results highlight nuanced challenges balancing innovation and cybersecurity. Recommended strategies within these limitations include access controls, professional standards, strong legal deterrents, public awareness campaigns, and robust network defenses. Ultimately, although directly policing open-source software is problematic, thoughtful multidimensional policies can still curb misuse while preserving liberties. This synthesis of technical, legal, and policy insights provides promising paths for wisely safeguarding society amidst rapid technological change.

Keywords: Wireshark, illegal access to network, data theft, cybercrime, policy regulation, packet sniffing, Philippine laws

INTRODUCTION

Background of the Study

Through the advancement of technology, the majority of the population has become aware of the use, convenience, and importance of technology. Businesses have gone online, having their transactions done digitally, and traditional monetary payments have switched to this trend as well. Not only has the private sector switched to this very convenient manner, but even the government has lots of considerations for online transactions due to their convenience, setting aside the emergence and threat of the COVID-19 pandemic (World Economic Forum, 2020). In an article written by Grzegorzek (2021), he explains that these technological advancements have been a breakthrough that has opened lots of new opportunities, as they have become an avenue for faster access to information, and a faster analysis and transfer of data. However, this advancement in technology and the opportunities it may bring to society, still pose some threat to its users.

It may be true that technological advancements bring convenience and faster transactions; however, according to The Asia Foundation (2022), people who have a vast range of knowledge in technology may be using this as a tool to take advantage of those who are engaged in it in terms of traffic analysis and information gathering. Data shows that the use of this technology has posed a huge concern for data breaches, fraud, identity theft, and other computer-related issues. In a report by Comparitech (2022), there

were 2.8 million fraud reports from consumers in 2021, a nearly 27% increase over the 2.2 million fraud reports in 2020. 26.4% of these were from people between the ages of 30 and 39, while just 4.7% were from people over 70 years old. This data shows that those who abuse technological advancement mainly target those at the age of 30 and above, however, in today's society, we must not forget that teenagers have now become targets of these abusers and this was further supported by a data from Statista (2021), where 22.4% of users are 18-24 years old·

What is more concerning is that the above-mentioned age group is being targeted by this technological advancement in a form of prank that may be threatening to the end-user. One of the commonly used tools for pulling these pranks is Wireshark.

Wireshark

Wireshark, which was previously known as Ethereal, is one of the most efficient tools that are used for traffic analysis (Alfawareh, n.d.), including latency issues, dropped packets, and malicious activity across the network (Malek & Amran, 2021).

They also added that there are many different functions and capabilities that Wireshark can perform, and anyone can use it, whether for good or bad intentions. This packet analyzer can be used to troubleshoot networking issues, record communications (e.g., email, voice, chat), record and analyze web traffic, reconstruct images, and even capture usernames, passwords, or personal information throughout the traffic.

In the present, this program can also be used by content creators who pull pranks on other people by directly telling them their names and even their exact location. It could be scary and threatening on the part of the end-user, as without even subscribing to anything, his or her private information is revealed to those who use this program. This can be done through packet sniffing and a packet sniffer.

Packet Sniffing and Packet Sniffer

Packet sniffing is the act of monitoring packets flowing through a network. Packets are basically data that is transmitted through a computer network (Malek & Amran, 2021). Packets may be stolen, intercepted, or attacked through a sniffer. Packet sniffing is a double-edged sword. On the one hand, it is an essential tool for network security professionals and digital forensics experts. On the other hand, it can be used for nefarious purposes by cybercriminals and hackers.

The sniffer is an application that performs the sniffing process. It is also called a network protocol analyzer.

A sniffer has two modes of operation: promiscuous mode and non-promiscuous mode.

Jeyanthi (2018) remarked that in promiscuous mode, the sniffer can steal information from the traffic passing over the network from all devices connected to the host network. On the other hand, the non-promiscuous mode can steal only the information going to and from its host system. He also added that the information that can be stolen by these sniffers is very sensitive, such as user credentials, including IDs and passwords, account details, network specifics, credit card numbers, email addresses, DNS, chat sessions, web pages being visited, etc. This information may be used to facilitate crimes that the user may not be aware of.

Statement of the Problem

While it is true that technological advancement does a huge favor for its users, it is still noteworthy to know that it is not only about the advantages as it also poses negative implications for its users when abusers come along.

This study primarily aims to determine how Wireshark packet sniffing can enable cybercrimes and be penalized under the Philippine law. It also examines limitations in regulating open-source software misuse.

Scope and Limitation

This study focuses on cyber threats from Wireshark packet sniffing, relevant laws, and recommendations to mitigate misuse given limitations in open-source regulation under the Philippine setting. Other cyber threats and software are outside the scope.

METHODS

This study conducted a literature review on Wireshark packet sniffing and related cyber threats. Interviews were also held with the Philippine National Police Anti-Cybercrime Group and National Bureau of Investigation—Cybercrime Division to understand challenges in regulating open-source software misuse.

LITERATURE REVIEW

An extensive review of literature was conducted to understand Wireshark packet sniffing and related cyber threats. Sources included journal articles, conference papers, tech reports, and textbooks on network monitoring, traffic analysis, cybersecurity, privacy, and cybercrime.

Overview of Wireshark Packet Sniffing

Wireshark is an open-source network protocol analyzer used for network troubleshooting, analysis, and security monitoring (Malek & Amran, 2021). It captures and logs traffic data packets flowing through a network using a packet capturing library like WinPcap (Jeyanthi, 2018). Wireshark can put network interfaces into "promiscuous mode" which taps into all network traffic, not just the host system's (The Ethics of Packet Sniffing, n.d.). This allows it to deeply analyze network performance.

However, promiscuous mode also enables capturing potentially sensitive information like usernames, passwords, device locations, emails, messaging data, web browsing history, and other personal details (Qadir et al., 2022). Mishra (2013) explains that sniffers like Wireshark can reconstruct web pages visited, images, files, and even some encrypted communications. All network traffic is exposed.

Cyber Threats and Legal Violations

Specific summary of cybercrimes and threats enabled by malicious Wireshark packet sniffing include:

- Data and privacy theft through illegal access or system interference, violating Philippine laws like RA 10175 Sections 4(a)1 and 4(a)4 (Jeyanthi, 2018). Stolen data facilitates further exploitation like identity theft, fraud, and additional network intrusions (Qadir et al., 2022).
- Distributed denial of service (DDoS) attacks which disrupt network infrastructure, like the overload of the Comelec websites during the 2016 Philippine elections (Macairan, 2016). DDoS employs traffic flooding.
- Disclosing individuals' personal information like names, locations, messages, and browsing data without consent for entertainment purposes (Instructables, 2016). This violates privacy laws as it captures and reveals data without authorization.
- General privacy violations by exposing confidential usernames, passwords, emails, web browsing activities, and other sensitive user information (Malek & Amran, 2021; Mishra, 2013).
- Enabling further cybercrimes like man-in-the-middle attacks through traffic monitoring, phishing through password theft, identity fraud through data capture, and malware injections into the network traffic flow (Qadir et al., 2022).

Analysis of Wireshark's capabilities and role in various cyber threats suggests that solutions require a synthesis of technical defenses, educational programs, ethical standards, and legal measures tailored to the unique challenges of open-source regulation.

Interviews

Semi-structured interviews were conducted with cybersecurity experts from law enforcement:

- Nova De Castro-Aglipay and Col. Arnel Hawthorne, PNP Anti-Cybercrime Group (PNP ACG)
- Attorney Ria Vanessa Asuncion, NBI Cybercrime Division (NBI CCD)

These agencies were selected due to their experience handling cybercrimes and expertise in technologies like Wireshark. Interviews were conducted via videoconference and lasted approximately 30-45 minutes each.

The interviews aimed to understand the challenges faced by law enforcement in regulating the use of open-source network monitoring and hacking tools like Wireshark. Questions focused on current laws, difficulties in enforcement, limitations in oversight of publicly available software, and potential solutions.

Experts were asked about their direct experiences handling cases involving packet sniffing cybercrimes, limits of existing legislation, gaps in practical enforcement, feasibility of restricting access to open-source tools, and recommendations for technology regulation given these constraints.

Responses highlighted the nuanced nature of balancing innovation and security in an unregulated digital landscape. Insights from frontline cybersecurity experts supplement the literature by providing real-world investigative perspective on legislating rapidly evolving technologies.

RESULTS

The literature review and law enforcement interviews conducted in this study reveal a complex landscape around Wireshark packet sniffing. On one hand, Wireshark enables invaluable network analysis through comprehensive traffic monitoring. However, the same capabilities also introduce risks of sensitive data exposure and criminal exploitations. Meanwhile, the open-source nature of Wireshark confounds direct regulation. These multifaceted results illuminate the nuanced challenges in balancing innovation and security.

Findings from the Literature Review

The comprehensive literature review provided crucial insights into both the invaluable capabilities and potential misuses of Wireshark packet sniffing. Key technical, legal, and ethical findings are summarized as follows:

1. Wireshark's capabilities for network troubleshooting, analysis and security monitoring through placing network interfaces into promiscuous mode to deeply monitor all traffic packets, not just the host's (Malek & Amran, 2021). This allows inspection of network performance.
2. However, it also enables capturing sensitive information like usernames, passwords, locations, web browsing history, and communication contents by assembling all exposed packets (The Ethics of Packet Sniffing, n.d.). Personal user data is jeopardized.
3. Specific examples of misuse include the 2016 Comelec website overload involving Wireshark, allegedly compromising the records of 55 million Filipino voters including names, addresses, and parents' details (Macairan, 2016). This demonstrates real-world harm.

4. Further cyber threats enabled are illegal access to data, interference through DDoS attacks, and unethical personal data disclosure, violating laws including RA 10175 Sections 4(a)1 and 4(a)4 which penalize privacy violations (Jeyanthi, 2018).

Given these threats that can originate from packet sniffing, they will violate Sections 4 a (1) and 4 a (4) of RA 10175 of the Cybercrime Prevention Act, which provides:

SEC. 4. Cybercrime Offenses. — The following acts constitute the offense of cybercrime punishable under this Act:

(a) Offenses against the confidentiality, integrity, and availability of computer data and systems:

(1) Illegal Access. – The access to the whole or any part of a computer system without right.

(4) System Interference. — The intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses.

Threats originating from packet sniffing were also discussed in the case of *Disini v. Secretary of Justice* when the court declared Section 12 of RA 10175, which covers the real-time collection data of law enforcement officers, unconstitutional.

The court discussed that computer data—messages of all kinds—travel across the internet in packets and in a way that may be likened to parcels of letters or things that are sent through the mail. When data is sent from any one source, the content is broken up into packets, and around each of these packets is a wrapper or header. This header contains the traffic data: information that tells computers where the packet originated, what kind of data is in the packet (SMS, voice call, video, internet chat messages, email, online browsing data, etc.), where the packet is going, and how the packet fits together with other packets. The difference is that traffic data sent through the internet at times across the ocean does not disclose the actual names and addresses (residential or office) of the sender and the recipient, only their coded internet protocol (IP) addresses. The packets travel from one computer system to another, where their contents are pieced back together.

Section 12 does not permit law enforcement authorities to investigate the contents of the messages and uncover the identities of the sender and the recipient.

Along with this discussion, the court agreed with Justices Carpio and Brion that when seemingly random bits of traffic data are gathered in bulk, pooled together, and analyzed, they reveal patterns of activities that can then be used to create profiles of the persons under surveillance.

The malicious use of packet sniffing that is penalized under Sections 4 a (1) and (4) can also be punished in relation to Section 29 of the Data Privacy Act of 2012, which provides:

SEC. 29. *Unauthorized Access or Intentional Breach.* – The penalty of imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00) shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored.

Moreover, these acts can also be penalized under Section 9 (c), (d), and (i) of Republic Act No. 8484, which provides:

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS |Volume VII Issue VIII August 2023

Section 9. *Prohibited Acts*. – The following acts shall constitute access device fraud and are hereby declared to be unlawful:

- using, with intent to defraud, an unauthorized access device;
- using an access device fraudulently applied for;

(i) **disclosing any information imprinted on the access device, such as, but not limited to, the account number or name or address of the device holder, without the latter's authority or permission**; (*emphasis added)*

Findings from Interviews

Expert perspectives from frontline cybercrime investigators provided grounded insights into the practical challenges of balancing innovation and security. Interviews with the PNP ACG and NBI CCD highlighted real-world limitations around legislating rapidly evolving publicly accessible technologies like Wireshark:

1. Open-source software like Wireshark cannot be easily regulated or prohibited given its public accessibility – anyone can download and access it (PNP ACG).
2. Laws can penalize those who use packet sniffing for cybercrimes but cannot restrict Wireshark itself as it has legal uses and is accessible by right (NBI CCD).
3. Innovative solutions are needed to curb misuse that do not violate the open-source nature, like professional standards and public education (PNP ACG & NBI CCD).

In the interview conducted with the Philippine National Police Anti-Cybercrime Group (PNP-ACG), they specifically mentioned that open-source software is available to everyone and cannot be regulated; you just have to download it, and you do not need to be a professional in cybersecurity or IT to use it. If it is regulated, it is only possible to regulate IT professionals but not the public. It was supported by the NBI CCD that the software itself is not the problem; it is the user who poses a threat when using those softwares.

PNP-ACG further added that open-source software is regulated abroad but not in the Philippines. You can find lots of tutorials on how to use open-source software; you can find anything about it on YouTube or even anywhere on the internet if you really want to know how to use it. Hence, it is impossible to really regulate the use of open-source software in the Philippines.

NBI-CCD then agreed to what the PNP-ACG said, as according to them, Wireshark is an open source, and we cannot limit its use. Generally, here (in the Philippines), it is not possible. The purpose of packet sniffing is for troubleshooting; the problem is that some hackers use it to check (with authority) other networks or network traffic so they can use the data. We could not limit or mitigate anyone who uses open-source software since it is their right to use anything for whatever purpose they want to use it for.

Moreover, Wireshark is not used for malicious purposes but for network troubleshooting and security analysis of certain networks. There is nothing wrong with using it as long as it is being used for the purpose it should serve and, of course, with ethical considerations. It is not something we could restrict; the purpose (prank) *per se* is not illegal. It is different from wiretapping, but the purpose is somewhat the same, which is to sniff or tap. It is within the users' rights to use open-source software, especially since the software itself is not illegal.

Packet sniffing can be employed in cybercrime investigations to find illicit behavior, including data exfiltration, malware infections, and phishing attempts. Investigators can track the flow of data and pinpoint the origin of an attack by examining network traffic. It is crucial to remember that when using packet sniffing as part of an investigation, legal procedures must be followed (The Ethics of Packet Sniffing, n.d.). However, since there were no complaints filed with the authorities, the legal procedures cannot go through.

DISCUSSION

Implications of Findings

The findings reveal a nuanced challenge in balancing innovation and security. Wireshark represents the double-edged sword of technology – while enabling network troubleshooting, its misuse threatens privacy and safety. However, policing innovation by restricting access to open-source software contradicts the unregulated spirit of the internet. Effective solutions must thoughtfully address this dilemma rather than simply clamping down on technological freedom and creativity.

The interviews with law enforcement highlight the practical difficulties in monitoring something inherently open. Yet the literature shows misuse can violate laws protecting data, access, and service. Hence cybercrime requires innovative thinking, not just stronger laws. Solutions should empower ethical responsibility, not stifle opportunities.

Recommendations must align legal strengthening with professional standards, public awareness, and restricted access in limited contexts. Regulation works alongside education, ethics, and better alternatives, rather than becoming roadblocks to progress. Overall, the findings suggest nuanced guidance, not blanket prohibitions, are needed to promote security and innovation.

RECOMMENDATION BASED ON FINDINGS

While it is true that the unethical use of packet sniffing, specifically Wireshark, is not *per se* illegal, it still poses a threat to the public. Public security must be considered at all times, especially if data or privacy are at risk. Hence, effective solutions require a multifaceted approach to curb packet sniffing misuse within the constraints of regulating publicly accessible software. Specific recommendations include:

1. Restricting network access in public areas like internet cafes, as suggested by PNP ACG interviews. For example, open-source downloads could be restricted and regulated in public internet cafes so users cannot access certain sites. An argument for this solution could be: How will you mandate the public internet cafes to restrict access to those sites? Will it not violate constitutional rights? The answer to this argument is that government departments, specifically the NBI and PNP, and even local government units should practice their constitutionally granted police power to implement this kind of regulation to prevent further threats to privacy and security as this creates friction against misuse.
2. Establishing professional standards and certifications for the ethical use of packet sniffing tools, like limiting usage to authorized infosec professionals per NBI CCD. As suggested by the PNP-ACG, one of the possible measures that could be taken is to determine the tools that can be used by white hat hackers because it is known that this software can be used for malicious purposes. For instance, if an individual's work is not related to network monitoring, they may not be allowed to use the software given its potential for misuse. This promotes accountability.
   It could be argued that this measure violates an individual's right to access open software applications. However, as emphasized by the Supreme Court in *Chavez v. Gonzalez,* the Internet, being unregulated, still needs to be regulated at the very least. This measure does not necessarily remove their right to access these kinds of software, but only limits them to professionals who use them for official purposes.
3. Strengthening laws and penalties surrounding related cybercrimes enabled by packet sniffing, rather than regulating the software itself directly. For example, harsher punishments for privacy and data violations identified in the literature. The legislative body could amend laws like RA 10175 to address gaps, though this is not currently a priority. This deters malicious activities.
4. Educating the public on responsible use of open-source network tools to raise awareness of privacy risks, as emphasized by both PNP ACG and NBI CCD interviews. For instance, government agencies could conduct continuous cybersecurity lectures to inform citizens of packet sniffing misuse threats.

This empowers citizens against misuse threats.

5. Developing alternative cybersecurity solutions that address vulnerabilities exposed through packet sniffing, making networks harder to breach. This compensates for limitations in restricting software access directly.

Ultimately, the constraints around policing publicly accessible software like Wireshark necessitate a complex, multi-layered solution set. While direct regulation of the tool itself is infeasible, thoughtful policymaking can still promote security amidst innovation. By combining targeted access controls, ethical oversight, consequential laws, proactive education, and robust cyber defenses, packet sniffing risks can be mitigated within the boundaries of an open digital ecosystem. Guidance must be nuanced, not repressive. With care, essential troubleshooting abilities, creative liberties, and individual rights can all be preserved – along with privacy and safety. Though challenges remain, this study illuminates promising paths forward. Ongoing research and open discussion around wisely balancing freedoms and protections can further strengthen resilience against those who would exploit our interconnectedness. The recommended synthesis of technical, administrative, legal, and social approaches creates a web of safeguards resilient against misuse of packet sniffing capabilities. Continued collaborative research and debate can help refine protective solutions while maintaining the core openness underpinning digital society.

CONCLUSION

No one can deny that a packet sniffer such as Wireshark is very useful as a network monitoring tool that helps capture traffic along their network and can troubleshoot network traffic issues. However, it is a double-edged sword that can be used for malicious purposes. By the act of sniffing, it can record communications (e.g., email, voice, chat), record and analyze web traffic, reconstruct images, and even capture usernames, passwords, or personal information throughout the traffic. These capabilities may result in more harmful acts such as data/packet stealing through system interference and distributed denial of service (DDoS) attacks. It can also be used for disclosing sensitive information through content creation on various platforms. These acts violate Sections 4 a (1) and (4) of Republic Act 10175, also known as the Cybercrime Prevention Act of 2012, and can be related to Section 29 of Republic Act 10173, also known as the Data Privacy Act of 2012, and Section 9 (c), (d), and (i) of Republic Act No. 8484, or the Access Devices Regulation Act of 1998.

Unregulated open-source software such as this one cannot be penalized by the authorities as everyone has access to it and it is within their rights to use it to their satisfaction, but since it is open source, it could be used in an unethical manner. Hence, the cycle of its unethical use is still occurring as the cause of more harmful attacks. Thus, the researchers suggested several recommendations to mitigate the harmful effects of the unethical use of packet sniffing, such as (1) restricting physical access to the network, (2) setting a professional standard for the use of open-source software, (3) stronger implementation of the law, (4) educating the masses, and (5) innovative approach in cybersecurity.

This study is focused only on the discussion of the unethical use of Wireshark as one of the many packet sniffers. Other studies that may be relevant to the theme and topic of this study are of the utmost importance in discovering other venues for arguments and other pertinent matters that need to be discussed.

REFERENCES

1. 30+ identity theft facts & statistics for 2022. (2022). Comparitech. https://www.comparitech.com/identity-theft-protection/identity-theft-statistics/
2. Alfawareh, M. (n.d.). *A deeper look into network traffic analysis using Wireshark*. Academia.edu – Share research. https://www.academia.edu/ 38418631/A_Deeper_Look_into_Network_Traffic_ Analysis_using_Wireshark
3. Chavez vs. Gonzales, G.R. No. 168338 (S.C. February 15, 2008)

4. Disini vs. Secretary of Justice, G.R. No. 203335 (S.C. February 11, 2014)
5. Global internet users age distribution 2021. (2021). Statista.https://www.statista.com/statistics/273018/percentage-of-global-internet-users-by-age-group/
6. GRZEGORZEK, J. (2021, June 7). The STEEPLE Analysis – Technological Opportunities and Threats. *Super Business Manager*. Retrieved August 9, 2023, from https://www.super business manager.com/the-steeple-analysis-technological-opportunities-and-threats/
7. Instructables. (2016, October 20). Omegle location prank with Wire Shark. https://www.instructables.com/Omegle-Location-Prank-With-Wire-Shark/
8. Jeyanthi, B. P. (2018). A review on various sniffing attacks and its mitigation techniques. Indonesian Journal of Electrical Engineering and Computer Science, 12(2502–4752).
9. Macairan, E. (2016, April 29). 2nd Comelec hacker nabbed. Philstar.com. https://www.philstar.com/headlines/2016/04/29/1577108/2nd-comelec-hacker-nabbed
10. Malek, M. S. A., & Amran, A. R. (2021). A study of packet sniffing as an imperative security solution in cybersecurity. Journal of Engineering Technology, 9(1), 96-101.
11. Mishra, V. (2013). Combating packet sniffing. International Journal of Information and Computation Technology, 3(10).
12. National Privacy Commission. (2022). NPC-SS-22-001 and NPC-SS-22-008-2022.09.22 In re Commission on Elections Decision Final. https://www.privacy.gov.ph/wp- content/uploads/2023/01/NPC-SS-22-001-and-NPC-SS-22-008-2022.09.22-In-re-Commission-on- Elections-Decision-Final.pdf
13. Philippine Daily Inquirer. (2022, January 12). In the know: The 2016 'Comeleak'. INQUIRER.net. https://newsinfo.inquirer.net/1570496/in-the-know-the-2016-comeleak
14. Republic Act No. 10173, Data Privacy Act of 2012 (2012).
15. Republic Act No. 10175, Cybercrime Prevention Act of 2012 (2012).
16. Republic Act No. 8484, Access Devices Regulation Act of 1998 (1998).
17. The Asia Foundation. (2022). Cybersecurity in the Philippines: Global context and local challenges. https://asiafoundation.org/publication/cybersecurity-in-the-philippines-global-context-and-local-challenges/
18. The Ethics of packet sniffing: Is it legal and ethical to sniff network traffic? (n.d.). LinkedIn. Retrieved May 8, 2023, from https://www.linkedin.com/pulse/ethics-packet-sniffing-legal-ethical-sniff-network-traffic
19. World Economic Forum. (2020, March 24). How governments are communicating online during the COVID-19 crisis. https://www.weforum.org/agenda/2020/03/government-coronavirus-covid19-communication-online-digital-technology/