Centre for Defence and Security Strategic Studies/
"Carol I" National Defence University, December 9-10, 2021

DOI: 10.53477/2668-6511-22-29

THE DEGRADATION OF HUMAN RIGHTS AND FREE PRESS THROUGH THE PEGASUS SOFTWARE IN THE ERA OF SURVEILLANCE, AS A THREAT TO INTERNATIONAL SECURITY. A DEBATE OF CIVIL LIBERTIES AND CENSORSHIP

Maria PÎRVU,
Student, Queen's University Belfast, Belfast, United Kingdom.
E-mail: mpirvu01@qub.ac.uk

Abstract*: The evolution of cyber spying technology presents new and rising dangers; coupled with the easy justification for use of the on-going terrorist crisis these dangers have now become major threats to the international security system. This article aims to provide analysis of these threats, using the new software Pegasus as a focal point of discussion. Developed by the Israeli 'cyber-warfare' company 'NSO', this spyware signals a danger not only to security but freedom of the press and journalistic integrity. This paper's focus will centre on how this software is used for censorship rather than to combat terrorism and will examine the social and political ramifications of said use. As highlight, the case of UAE activist Ahmed Mansoor and his contemporaries who were writing against authoritarian governments will be discussed. This article will urge that strict global legislation is needed to stop the abuse of spyware as a tool of censorship.*

Keywords*: security threat; NSO Pegasus; censorship; citizens' rights; counter-terrorism activism; free press; spyware.*

Introduction

George Orwell's dystopian world of 1984 is famous for the quote "Big Brother is watching you" (Orwell 1949, 3). Although his work has always been considered fiction, the ongoing change of reality proves that we might not be so far from his imaginative world. The spying industry has been merged in the last decades with the world of cyber technology. New alternatives have risen to protect the integrity of the international system, but so have the dangers that could compromise it. Among the most recent ones that surfaced is Pegasus, which was developed by the Israeli company NSO. A powerful and discreet tool, NSO promises that the mission of this spyware is to counter terrorism and crime, however, the recent events reveal that it has been used in other ways as well, some of them being unethical, and potentially illegal.

This article aims to provide a starting point, a warning signal of the rising security issues that Pegasus exemplifies. Through presenting how it operates, examining the threat posed by its advanced technology and distinguishing the main issues that arise from its use, this article becomes a framework for this new potential danger. Specific examples from recent events of potential issues that can arise from its use will be provided for every argument. This article will have a political, legal, and ethical approach on the issue of the Pegasus spyware and will culminate with some recommendations on what should be done in the international system to prevent any security disruption, actions that have already started to happen.

1. Pegasus: an analysis

1.1. What is Pegasus?

The landscape of cyber security is one defined by perpetual evolution, to every new firewall or antiviral software, there is an equivalently new type of malware or backdoor. Due to our modern reliance on technology, cyber threats can fundamentally alter our private and

public safety; these can pose dangers to the individual but have ramifications to the wider world of international security and public liberty. These types of malicious software, like Pegasus, intentionally damage a device or network by penetrating through the internet, email, or text messages, for example hiding under the form of an application, which the victim unknowingly installs. There is a wide variety of malware, such as computer viruses or, in the discussed case, spyware. The Federal Trade Commission (2021) in America defines spyware as "*one type of malware that can monitor or control your computer use*." Once installed in the device, it can be used to monitor the computer's activity, get access to private data and personal information, which can result in fraud commission, identity theft, or the stealth of personal data for various purposes.

The organisation that developed Pegasus is the private Israeli company NSO. In the last decade, this private group has been the focus of international scrutiny. The company describes itself as an ethical organisation that supports government bodies by providing their powerful software in order "to prevent and investigate terror and crime" (NSO Group, 2021), a noble goal. Publicly, their addressing of criticisms levied against that their software has been unethically used is sparse, furthermore, it cannot be found anywhere on the website any information about 'Pegasus', which is their invention, as well as the centre point of the entire scandal, which strengthens scepticism for their true intentions.

The Pegasus software is a spyware trojan that can penetrate any mobile device and access any type of data it owns. It can only be used on mobile smartphone devices and can infect all types of operating systems. It has unlimited access to the target's device and is used to collect all the data a mobile infected possesses. This article will use Amnesty International's (2021) forensic report as a framework on how Pegasus operates. This framework lays out the stages by which Pegasus attacks a device to extract information. The first stage of infection is targeting a device. A link is sent to a smartphone, usually through either SMS or WhatsApp.

From here on, the process remains the same as other software infections, the spyware installs itself and starts accessing everything on the device. Once it penetrates the device all information on it is compromised. It hides as operating systems processes, which makes it much harder to be identified. For example, on the IOS devices, "*most Pegasus process names seem to be simply disguised to appear as legitimate iOS system processes, perhaps to fool forensic investigators inspecting logs.*" (Amnesty International 2021, 27). The final stage is the tracking, as the spyware sends all the data and information accessed on the device to a third party operating in a secret manner that can use it to monitor the victim's life. The information acquired could potentially be used against the target with possibly massive implications to that person and the organisation they are associated with.

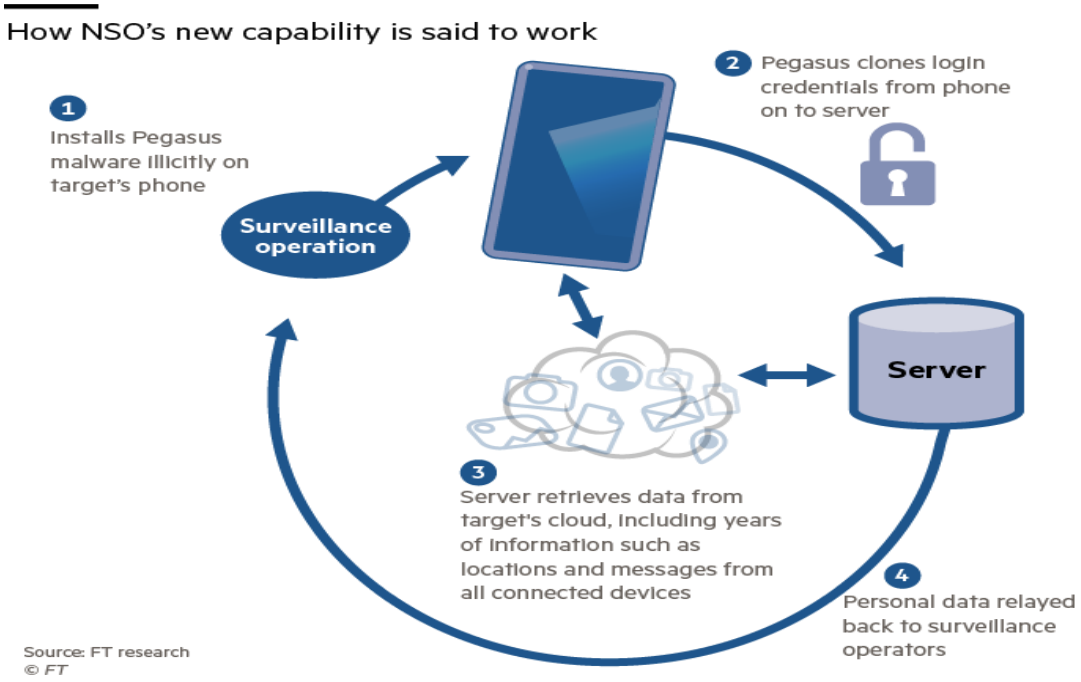

Figure no. 1: Financial Times Research, 2019.

The Pegasus project was created to investigate NSO's actions with Pegasus, and to reveal its abusive use around the world. It is an ongoing international investigative journalism project, initiated by Forbidden Stories (a French media non-profit organisation) and Amnesty International (a non-governmental human rights organization) to conduct forensic analysis over the use of Pegasus. A various number of newspaper agencies, as well as independent journalists around the world, are part of the project and aim to uncover that Pegasus is used not only for its presented purposes. Since 2016, The Pegasus Project unfolded the story of the spyware, identified a leak of more than 50,000 phone numbers that were infected and targeted by the Pegasus software and exposed the use of the spyware in India, Morocco, Italy, Mexico, Saudi Arabia, Hungary, United Arab Emirates and Azerbaijan. Among the phone numbers targeted, human rights activists, leading opposition politicians, lawyers, journalists, and political dissidents were identified. In 85% of the phone numbers targeted, the mobile phones were infected with spyware. (Forbidden Stories, 2021) Their analysis progressively concludes the spyware was used by authoritarian or flawed democratic government bodies to spy on individuals that can be a potential risk to their governance. The investigation will be the starting point for elaborating all arguments in this paper.

1.2. Why is it so dangerous?

This is a powerful tool, but it is especially dangerous for two reasons, firstly the aforementioned 'zero-click' technology and secondly NSO's nature as a non-government private organisation. Immediately Pegasus stands apart from many of its contemporaries as it uses a 'zero-click' technology, which enables it to access the mobile device without the user knowing it at all and leaves no traces of it being on a smartphone. It works by identifying any security breaches and flaws in the operating system or apps and using them to infiltrate the device. This represents a technology that is much harder to track, meaning that it becomes much less detectable to discover. "The technical effort required to identify cases markedly increases, as does the logistical complexity of investigations." (Marczak, Scott-Railton, Al-Jizawi, Anstis, and Deibert, 2020, p. 16). This technology could evolve to a point where it can no longer be identifiable, which leaves devices completely vulnerable to spyware and compromised privacy.

Furthermore, in a similar way to American mercenaries not being reported in war statistics, a government's use of outsourced private spyware does not have to be reported and can remain anonymous and untraceable between the company and the government. Currently, the private sector, particularly corporations, can only be prosecuted under national law by a state if it infringes any human rights. This means that the corporate responsibility for ethical and social issues is left to be self-regulated, which can be a detriment to the transparency and accountability in the private sector. Only sovereign states and other entities that are legally recognized as international actors can be subjected to international law. As a result, government bodies can 'hack' international law, not be held accountable for using this spyware. This lack of accountability could result in human rights abuses, such as the privacy right. There are only just a few international organisations that aim to act as guidance against human rights abuses in the private sector, such as "*United Nations Guiding Principles on Business and Human Rights", "United Nations Guiding Principles on Business and Human Rights, "Company Codes" and "Alien Tort Statute* (Yadav 2020, 370-371). Ultimately, this lack of regulation maintains the privacy of those who might use the spyware. Therefore, when NSO sells the use of its software and it may be used in an abusive manner without accountability, it is easy therefore to see that these principles can be applied to not only domestic surveillance but international ones. Exposing private secrets can have massive political implications and can undermine trust by building an atmosphere of ever-present danger and mistrust, which can culminate in the disruption of international security.

In this way, the existence of software such as Pegasus is a major contributor to the cybersecurity dilemma, which can be a bigger risk to international security. Nicholas C. Rueter (2011) argues that because of the nature of cyberwarfare, the cybersecurity dilemma may be more complicated to overcome than the normal security dilemma. He illustrates the cybersecurity dilemma as a chain reaction of cross-national digital security. A state increasing its digital infrastructure's security by strengthening its defensive or offensive cyberwarfare can lead to the degradation of others. Pegasus creates an unstable atmosphere in the international system. States know that the spyware exists, and other government bodies can use it, which can determine them to strengthen their cyber-security. "*An attacker who does not burrow himself deeply into opponents' cyberspace risks having an empty arsenal when a conflict occurs*." (Kello, 2017) The Pegasus project has revealed that among the leaked phone numbers that were infected with Pegasus, 14 world leaders were identified[1]. It has not been confirmed who coordinated the operations against these world leaders, but if NSO stated that it sells the spyware to governments bodies, it can be deduced that government bodies have used it against these world leaders. This can progressively decrease the mutual trust in the international community, ultimately, the possibility of a conflict may arise.

From an ethical perspective, states who use Pegasus violate the social contract, decreasing the legitimacy of their sovereignty. It is undoubtedly clear that a functioning society is based on the social contract theory, which particularly is the justification of power that law enforcement can exert over the population in exchange for security. Citizens give up some of their freedoms to become a collective secure society governed by the rule of law. Just as John Loke (1689) argues, the power of consent is the most important factor of the social contract. For governments to use the Pegasus spyware for surveillance means that individuals are unable

[1] A.N.: Cyril Ramaphosa (the president of South Africa), Emmanuel Macron (the president of France), Tedros Adhanom Ghebreyesus (WHO's director general), Saad Hariri (former prime-minister of Leabon), Charles Michel (the president of the European Council), Mohammed VI (King of Moroco), Saadeddine Othmani (Moroco's prime-minister), Imran Khan (prime-minister of Pakistan), Felipe Calderón (former president of Mexico) and Robert Malley (American diplomat). For further detail, see (Chrisafis et al. 2021), URL: https://www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data

to assert consent, which, ultimately, leads to governments not being subjected to the rule of law. This can lead to breaches in the social contract, particularly, states not being held accountable for their actions, which can weaken a democratic state. The power of consent is cancelled by the violation of the right to privacy, as "The governors and the governed should be subject to the law." (Taylor 2002, 66).

2. The right to privacy in democratic and authoritarian regimes under the influence of Pegasus

There are many threats the Pegasus spyware imposes to the international security, however, the biggest one and the most investigated one is democracy. By having such a state-of-the-art spyware technology, especially unregulated, governmental bodies in democracies can use it to infringe the human right of privacy or break the fundamentals of democracy.

International human rights law covers the right to privacy in multiple conventions, such as 'International Covenant on Civil and Political Rights (1976, Article 17)', 'Convention on the Rights of the Child (1990, Article 16) International Convention on the Protection of All Migrant Workers and Members of Their Families (1990, Article 14) (United Nations 2021) As highlighted in the universal rights declaration,

"*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*." (United Nations, 1949, Art. 12)

The use of Pegasus violates all the conventions mentioned above, firstly because it operates a 'zero-click' policy, which does not enable the target to consent at all and represents a new and much more dangerous implication in spyware. This, coupled with the core idea that spyware is an intrusion of the international right to privacy become drivers of how dangerous this new spyware is to the international security.

Not only the use of Pegasus violates one of the most basic human rights, but it can weaken democracies, especially when governments are able to not be held accountable. It can do this by being a contributor to the establishment of various actions over time that can detriment the democracy of a state. An illustration of this argument can be exemplified by the use of Pegasus in Hungary. It has been confirmed that out of the 50,000 leaked phone numbers that were targets of the spyware, Hungarian journalists, media owners and political figures were confirmed victims of Pegasus. (Marczak, Scott-Railton, McKune, Abdul Razzak, and Deibert 2018, 15) The legislation in Hungary allows the government to operate mass surveillance operations on individuals who are not related to any investigations, nor are under suspicion on any law breaches. For this to happen, in the case of an attack of the state's national security, intelligence gathering services can operate without a judicial oversight, without an external assessment, only with the approval and signature of the justice minister. Judit Varga, Hungary's justice minister recently "*has declined to comment on whether the Hungarian government uses Pegasus, but said "every country needs such tools*" (The Guardian, 2021) The justice minister's statement belies a disregard for a fundamental principle of democracy, the separation of the powers of the state. The mere existence of Pegasus spyware in Hungarian journalists, lawyers and opposition politicians is a direct violation to the right of privacy, coupled with the possibility of the government using it become a serious threat to the democracy in Hungary, especially due to its shaken times as a democracy.

Furthermore, authoritarian states can use the spyware to consolidate their regime and to strengthen their control over the population. This added power weakens both the chance of them becoming democratic and the international security. Totalitarian governments are maintained and expand through crushing or discrediting their opposition. In the past, authoritarian governments could have been held accountable for abusing human rights on

political dissidents as there was some physical component, violating the rule of law and being under trial at the Supreme Court in the end. However, the Pegasus software allows authoritarian governments to escape this accountability. NSO is a private company with no obligations to disclose who uses their service. The Citizen Lab's 2018 study revealed examples of authoritarian governments used Pegasus to spy on political dissidents, human rights activists, lawyers, and journalists from 2014 to 2018. This is additional proof that Pegasus can contribute to abuses in the international security.

Table no. 1: Reported cases of individuals targeted with NSO Group's Spyware (Marczak, Scott-Railton, and Deibert 2018, 10)

Country Nexus	Reported cases of individuals targeted	Year(s) in which spyware infection was attempted
Panama	Up to 150 (Source: Univision)[1]	2012-2014
UAE	1 (Source: Citizen Lab)	2016
Mexico	22 (Source: Citizen Lab)	2016
Saudi Arabia	2 (Source: Amnesty, Citizen Lab)	2018

Table 4: Reported cases of individuals targeted with NSO Group's Spyware

Among the individuals targeted by Pegasus, the 51 years old engineer Ahmed Mansoor, appears to be a significant victim, as he is a renowned figure in Middle East and North Africa region, admired for his close implication in human rights activism and criticism of the UEA government. In 2016, he received a text message that claimed to reveal secrets of the tortured prisoners in the UAE if he clicked on the link provided. Ahmed Mansoor forwarded the message to The Citizen Lab and, together with Lookout Security started an investigation. It was concluded that the link contained Pegasus spyware and the operation of attempting to infect his phone was correlated with the UAE Government.

"The attack on Mansoor is further evidence that "lawful intercept" spyware has significant abuse potential, and that some governments cannot resist the temptation to use such tools against political opponents, journalists, and human rights defenders." (Marczak and Scott-Railton 2016, 3).

3. (Not so) free press?

Pegasus becomes an issue of concern in the media world as well, as such spyware is a contributor to the degradation of both free and independent press. Around 180 journalists were targets of NSO Pegasus and the investigations linked different authoritarian governments to the spyware's infection of journalists. (IPI-Admin 2021) Such actions can be a direct infringement of democratic fundamentals, particularly freedom of expression and free and independent press.

The Pegasus spyware is a contributor to the creation of a chilling effect in the international media, as an immediate reaction which, ultimately can lead to censorship of independent media in the long term. The chilling effect can be defined as a "*negative deterrence of communication: that a person or organisation is made physically colder by inhibiting the exercise of their right to free expression*" (Townend 2017, 73) It represents a consorted effort of repression through legal and non-legal means by a regime that aims to limit the exercitations

of the individual's right to free speech. In this context, the acknowledgement and use of the Pegasus spyware can discourage media agencies and journalists to critically engage with governmental actions due to a fear of becoming a victim. It becomes an intimidation tool that can lead to an auto-censorship. Just as the separation of powers regulates the state in a democracy, critical and free media has a significant contribution to influencing government authority over the population. Compromised independent media is not only an infringement of the right to free speech, but also a factor that weakens the quality of a democratic state and strengthens the power in an authoritarian one. In the long term, the use of Pegasus as a tool to create a chilling effect can result in a rise of prominent censorship in the international media. When governments target with the Pegasus spyware independent journalists and media agencies, the process of censorship can happen in a much more discreet manner, which means it can be more effective and efficient.

During their forensic research at Amnesty International, John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert (2018) revealed that the Pegasus spyware has been repeatedly used on 8 Mexican journalists and, in some cases their family. They highlight that the journalists have been targeted with Pegasus just before or after the killing of a colleague or family member. Just a few days after the murder of Javier Valdez, a Mexican independent journalist, his wife Griselda Triana (who is also a journalist) fell as a victim of the Pegasus spyware, along with another attempt to infect two of his colleagues' phones, Andrés Villarreal, and Ismael Bojórquez. This strategy of targeting close contacts is an illustrator of the rise of the chilling effect through the Pegasus spyware, which can result in journalists auto-censoring themselves due to a fear of becoming victims themselves, or to put their family, friends, and investigations at risk.

4. What should be done?

Because the Pegasus spyware is so dangerous, immediate action needs to be taken. It represents only the beginning in the evolution of incredibly powerful surveillance mechanisms. The first step that needs to be taken to protect the international security is the adoption of a social norm against the Pegasus spyware, which is already happening. Precisely, first, the acknowledgement that the Pegasus spyware is used as a tool to censorship and human rights abuses as well, not only to combat terrorism and crime. Media coverage and public information is needed for this step to be complete. The Pegasus Project became a starting point of media coverage that urges the public to be informed that NSO is a potential threat to the international security. From here, public information can lead to criticism, which can lead to protests against NSO's actions, such as the Protests in Hungary on the 26th of July (Reuters, 2021). This, coupled with Pegasus being a threat to states' security as well, (like government officials being targets) can push the social norm into international consideration and governmental action.

When the social norm against private spyware technology is considered by international organisations it transforms itself into an international norm. This means that governments and international organisations start treating this as a security issue. When this happens, international action can be taken to push back against authoritarianism and for the protection of the rights. Official national investigations need to start to confirm who used the spyware in an abusive manner, so that the truth and clearance can be surfaced. If it will be confirmed that Pegasus was used in unlawful ways, the Israeli government needs to tighten its law around cybersecurity and to held accountable the NSO group for democratic and human rights violation.

If there is enough evidence that NSO's actions were unlawful, international organisations need to urge a change in the international law. The first and most important change in international law is that corporate surveillance companies should be subjected to

international law just like state actors, to ensure NSO can be held accountable for its actions at the International Court of Justice. The international law on espionage currently "either fails to regulate spying or affirmatively permits it" (Deeks, Abebe, Andrias, Cohen, Cordero, Daskal, Kaye, Kendrick 2014, 300) Especially in the cyber espionage area, because international law faces such an impediment, international organisations should encourage states to tighten their national legislations. Before approval, espionage cases should be reviewed and either approved or declined by an independent body within a state. The United Nations Office of High Commissioner (2021) have also urged to the establishment of a global moratorium as an immediate reaction to The Pegasus Project's revelations on the use of surveillance technology until regulations are put in place that follow international human rights standards.

The legislation must also focus on robust notice and consent requirements of spyware by the immediate ban of the 'zero-click' technology. To preserve a secure cyberspace, international organisations should encourage corporate technological companies to use safer ways of encryption, such as the quantic encryption, which is currently almost impossible to be broken.

Conclusion

The spyware technology in the international security world has brough many debates, in terms of its use from an ethical, technological, and political perspective. This article provided an analysis of the rising danger of spyware in the international system, with an emphasis on the Pegasus software developed by NSO. Particularly, how the Pegasus software is different and more dangerous than other tools of spyware and how it affects the international system. By using the information 'The Pegasus Project' provides as a framework, this article argued that the use of this spyware represents a great danger. Firstly, because it becomes a contributor to the process of damaging democracy and simultaneously to the process of strengthening authoritarian regimes around the international scene. Secondly, because it infringes both human rights, like the right to privacy and citizens' rights, like the detriment of freedom of expression by the creation of a chilling effect that promote censorship.

This article laid the groundwork for this new and rising threat and provided an analytical study of the most pressing and dangerous threats this new technology can do. Because this was a starting point of a few of the most dangerous threats Pegasus offers, further elaboration can be done on how NSO's Pegasus can be a contributor to a decrease in a states' security monopoly, which can lead to corporatocracy, about how such spyware can be done in an ethical way, on how the Israeli government should address this issue, or how the impact of Covid-19 digitalisation influenced the evolution of this spyware.

The Pegasus spyware therefore becomes less of a useful help for combating terrorism and crime, but rather a contributor to the unsettlement of the international scene, by contributing to the security dilemma, promoting censorship, and unfairness. Immediate action at a global level needs to be taken, as such technology can shake the global political stage from its core and unpreceded consequences will be seen if no action will be taken. The new challenges of the international technological security world will be increasingly difficult, but so must be the political actors to face them.

BIBLIOGRAPHY:

Amnesty International. 2021. "Forensic Methodology Report: How to Catch NSO Group's Pegasus." Amnesty International. Peter Benenson House, 1 Easton Street London WC1X 0DW, UK: Amnesty International Ltd. Available at: https://www.amnesty.org/en /latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

C. RUETER, Nicholas. 2011. "The Cybersecurity Dilemma." Master Thesis. Department of Political Science in the Graduate School of Duke University. http://docplayer.net/957458-The-cybersecurity-dilemma-nicholas-c-rueter-department-of-political-science-duke-university-date-approved-alexander-downes-supervisor.html

CHRISAFIS, Angelique, Dan SABBAGH, Stephanie KIRCHGAESSNER, and Michael SAFI. 2021. "Emmanuel Macron Identified in Leaked Pegasus Project Data." The Guardian. July 20, 2021. https://www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data

DEEKS, Ashley, Daniel Abebe, Kate Andrias, Harlan Cohen, Carrie Cordero, Jen Daskal, David Kaye, and Leslie Kendrick. 2014. "An International Legal Framework for Surveillance." https://www.ilsa.org/Jessup/Jessup16/Batch%202/DeeksLegal Framework.pdf

Federal Trade Commission. 2021. *Spyware and Malware*. <https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/spyware-and-malware> [Accessed 8 September 2021]

Financial Times Research. 2019. *How NSO's New Capability Is Said to Work*. https://www.ft.com/content/2f5feb53-e7ff-47b3-ad42-93a8f2bc6aac

Forbidden Stories. 2021. "About the Pegasus Project | Forbidden Stories." Forbiddenstories.org. 2021. https://forbiddenstories.org/about-the-pegasus-project/

General Assembly, United Nations. 1949. *Universal declaration of human rights* (Vol. 3381). Department of State, United States of America.

IPI-Admin. 2021. "Pegasus Project: Full Investigation Needed after 180 Journalists Targeted by Spyware." International Press Institute. July 19, 2021. https://ipi.media/pegasus-project-full-investigation-needed-after-180-journalists-targeted-by-spyware/

KADAM, Munmun, and YADAV Rahul. 2020. "Corporate Accountability and human rights violation". Volume I. Issue II. April 2020.

KELLO, Lucas. 2017. "The Security Dilemma of Cyberspace: Ancient Logic, New Problems." Review of *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations*, by Ben Buchanan. https://www.lawfareblog.com/security-dilemma-cyberspace-ancient-logic-new-problems

LOCKE, John. 1689. "Two Treatises of Government". 1st edn. England: Awnsham Churchill. (chapter 2-19)

MARCZAK, Bill, and SCOTT-RAILTON John. 2016. "The Million Dollar Dissident: NSO Group's IPhone Zero-Days Used against a UAE Human Rights Defender."

MARCZAK, Bill, SCOTT-RAILTON John, MCKUNE Sarah, RAZZAK Bahr Abdul, and DEIBERT Ron. 2018. "HIDE and SEEK Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries." *Citizen Lab Research Report No. 113, University of Toronto*, September.

NARAYAN, Rahul. 2021. "Don't Let Pegasus Convert Citizens into Docile Bodies." *Mint*, June 30, 2021. http://14.139.58.147:8080/jspui/handle/123456789/4078

NSO Group. 2019. “NSO GROUP - Cyber Intelligence for Global Security and Stability.” NSO Group. 2019. https://www.nsogroup.com/

Office of the High Commissioner, United Nations Human Rights. n.d. “OHCHR | International Standards.” Www.ohchr.org. Accessed September 16, 2021. https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx

Office of the High Commissioner, United Nations. 2021. “OHCHR | Spyware Scandal: UN Experts Call for Moratorium on Sale of ‘Life Threatening’ Surveillance Tech.” Www.ohchr.org. August 12, 2021. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27379&LangID=E

ORWELL, George. 1949. *1984*. Harlow: Pearson Education.

Reuters. 2021. “Hungarians Protest against Alleged Illegal Surveillance with Pegasus Spyware.” *Reuters*, July 27, 2021, sec. Europe. https://www.reuters.com/world/europe/hungarians-protest-against-alleged-illegal-surveillance-with-pegasus-spyware-2021-07-26/

SCOTT-RAILTON, John, MARCZAK Bill, ANSTIS Siena, RAZZAK Bahr Abdul, CRETE-NISHIHATA Masashi, and, DEIBERT Ron. 2018. “RECKLESS vi Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague.” *The Citizen Lab*. University of Toronto: Citizen Lab Research Report No. 116. https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/

TAYLOR, Nick, 2002. State surveillance and the right to privacy. *Surveillance & Society*, *1*(1), pp.66-85.

TOWNEND, Judith, 2017. Freedom of expression and the chilling effect. In *The Routledge Companion to Media and Human Rights* (pp. 73-82). Routledge.

WALKER, Shaun. 2021. “Call for Hungarian Ministers to Resign in Wake of Pegasus Revelations.” The Guardian. July 28, 2021. https://www.theguardian.com/news/2021/jul/28/call-for-hungarian-ministers-to-resign-in-wake-of-pegasus-revelations