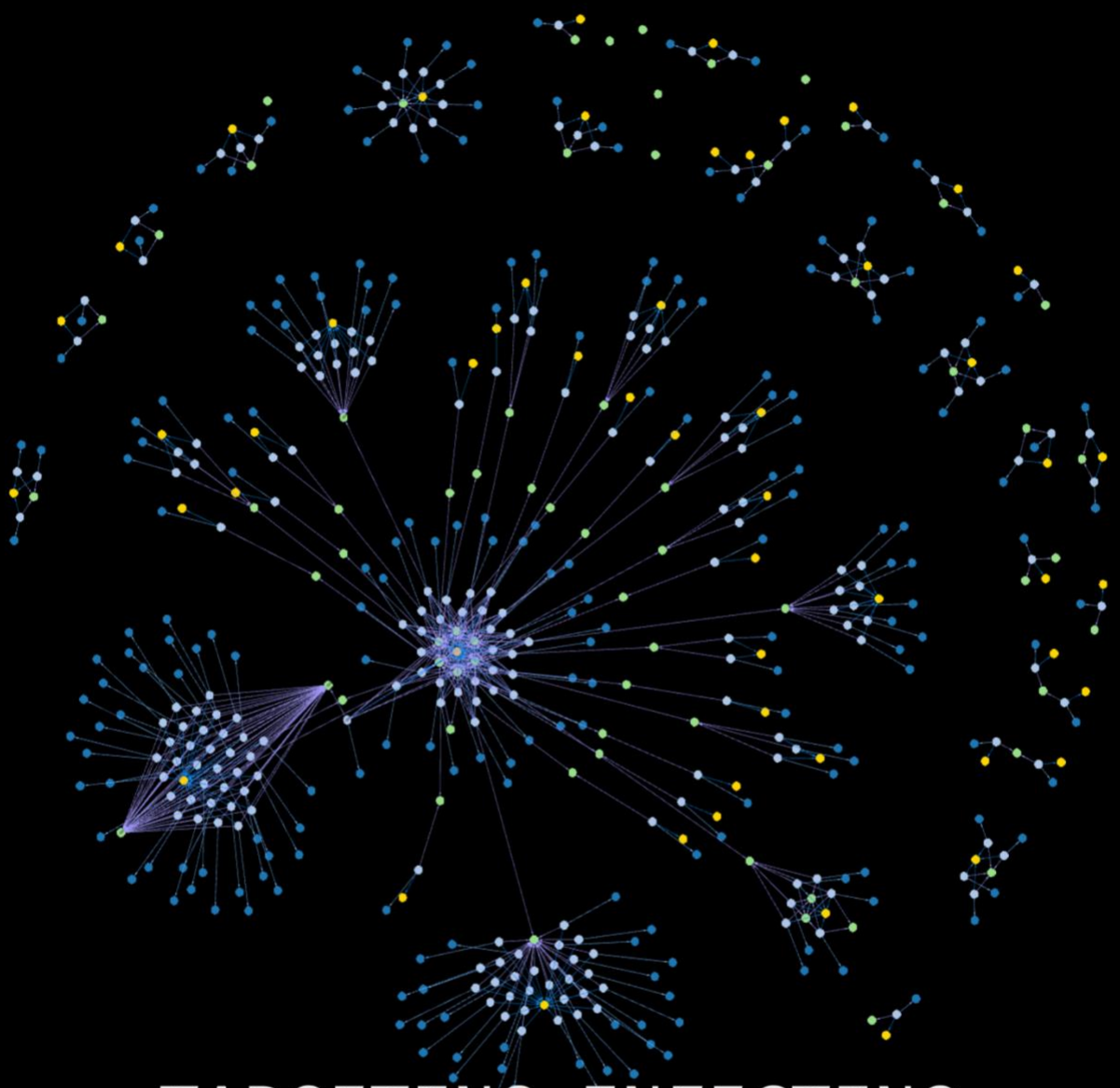
Geneva Graduate Institute
CyberPeace Institute



TARGETING, INFECTING SURVEILLING, HARMING

Aditi Kekre
Maira Cardillo
Sina Fischer

A Criminal and Human Rights Context:
Mapping the Impact and Harm of Spyware on People

Final Report, 07.07.2023

Targeting, Infecting, Surveilling, Harming

A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People

Authors

Maira Cardillo, Sina Fischer, Aditi Kekre

This report is the final output of the applied research project titled "ARP_2_02: A Criminal and Human Rights Context: Mapping the impact and harm of spyware on people". The project was hosted by the Geneva Graduate Institute in partnership with the CyberPeace Institute.

Acknowledgements

We would like to deeply thank our academic supervisor Dr. Bugra Güngör for his invaluable academic guidance and necessary critique, which has enabled us to comprehensively and efficiently bring this project to its completion. We would like to especially thank our tutor Mr. Mohammadreza Eghbalizarch for the extensive mentorship, tireless availability, and invaluable feedback throughout the 5-month research project, without which we would have been much more lost and much less happy. We would also like to express sincere appreciation to the CyberPeace Institute team, especially Ian Bowden and Nedelcho Mihaylov, for their guidance, keen support and enthusiasm towards us and the project, which has made the partnership incredibly fruitful and enjoyable.

Table of Contents

List of Figures

I. Executive Summary

The research project aims to analyze the human and societal impacts of spyware across the world in order to categorize and assess the scale of harm caused by spyware. The objective is to map the emerging trends of digital surveillance and gap the bridge of current research through the systematic collection of data. The results that have emerged are summarized below:

Quantitative analysis: The data set records 53 events over the course of 10 years, from 2013 to 2023:

- The highest number of events are observed in the regions of Central America (12 events), Western Asia (12 events), and Western and Southern Europe (10 events). The majority of events are recorded in Mexico (11 events).
- With 42 events, most of the spyware attacks are conducted by NSO Group's Pegasus software and the majority of attacks are inflicted by Zero-Click Exploits (55%). Governments are the primary customers of spyware (57%).
- Of the 216 identified targets, over 80% of the targets belong to the sectors of Advocacy, Media, and Politics. The majority of all targets are El Salvadorian followed by Spanish and Thai nationalities. 53% of the targets are male, whereas 25% are female.

Harm assessment: Cyber harm is defined as the detrimental consequence of a cyber-event affecting the individual's welfare interests.

- Of the recorded 216 targets, 164 individuals' digital devices are infected. 17 targets are experiencing severe psychological harm, most notably fear, anxiety, insecurity, a feeling of paranoia, loss of trust, and isolation.
- 8 targets are suffering from physical harm often relating to the prosecution, detention and imprisonment of targets. 6 targets including journalists, lawyers, priests and human rights defenders are experiencing financial harm within their professions due to a spyware attack.

Case studies: Three case studies (Spain, Western Asia and Mexico) demonstrate the long-term harm spyware harbors on specific target groups in the context of shrinking civic space, the erosion of free speech, and the suppression of opposition politics.

- They specifically shed light on how spyware abuse is directed towards individuals and groups engaged in dissent. The pattern further shows that spyware infiltrations are part of comprehensive attacks, including arrests or detentions before or after the digital surveillance, smear campaigns, and expulsion or isolation of the targets within their communities.

II. Introduction

Catalan leftist politicians (Deibert et al., 2022), Italian human rights lawyers (Campbell & D'Agostino, 2022), Moroccan journalists (Amnesty International, 2019b) and Togo priests (Scott-Railton 2020) are all facing the same issue: Extensive surveillance of their digital devices through spyware in reaction to their dissenting opinions, often executed by their own governments. While surveillance tactics and oppressive states are not new, the market for digital spyware has grown exponentially in recent years and is responsible for major human rights abuses globally.

The spyware market has extensively grown alongside the ever increasing development of digitalization. While new technologies are commonly produced to positively increase the quality of life, they also harbor the potential to be abused. The encapsulation of daily life in portable devices, such as smartphones, results in very powerful spying tools. The fast pace of new inventions has also resulted in a lack of regulatory frameworks for the selling and buying of spyware between states, intelligence agencies, and private cybersecurity companies (Shrivastava & Kejriwal 2021, Chan 2018). As the past years have shown, it is often in the interest of state institutions and companies to keep the market unregulated as they tend to profit from the lack of transparency and supervision (Guterl 2022).

Findings of leading research institutions have shown a staggering amount of spyware targets in the past ten years (Deibert et al. 2022, Guterl 2022). Intelligence services and militaries buy spyware packages from private security companies to target, infect and surveil dissidents, opposition leaders, human rights activists, lawyers, journalists, and other people who are gaining unfavorable political traction (Rueckert 2021, Guterl 2022). In Morocco, for example, the two human rights defenders Maati Monjib and Abdessadak El Bouchattaoui were targeted multiple times between 2017 and 2019 with spyware developed by NSO Group, an Israeli cybersecurity company (Amnesty International, 2019b). Both defenders were previously accused of various transgressions ('threatening internal security') by Moroccan authorities for criticizing repressive mechanisms of the state and supporting the protection of journalists' privacy (ibid.). Amnesty International was able to track and analyze both infiltrations which used SMS messages containing malicious links previously used by NSO Group (ibid.). Considering that Morocco had formerly intercepted phones of and intimidated freedom of expression of journalists, it is highly likely that these attacks were, if not executed, then approved by Moroccan authorities (Mansour 2021).

The harm that is done to the individual, but also to the whole community, may potentially be immense. Those targeted often face detention, imprisonment, defamation campaigns or, in extreme cases, assassination, following extensive digital surveillance (Deibert et al. 2022, Campbell & D'Agostino 2022, Amnesty International 2019b, Scott-Railton 2020, Human Rights Watch 2021). Additionally, the victimization through spyware use often leads to a feeling of paranoia, shame, guilt, and isolation (Fakih 2022, Guterl 2022). Communities at large further face the chilling effect on free speech and the undermining of democratic values.

This study, undertaken together with the CyperPeace Institute, will add to their current research series *"The Spyware Market Unpicked"*. **The study involved the systematic collection of data to analyze the impacts and harm of spyware abuse around the world.**

The following report engages with the following research questions:

- Who are the targets of spyware and which spyware tools have been used against them?
- Who are the customers of spyware tools and where do they deploy them?
- How have the reported incidents harmed the victims and how can the adverse effects be categorized and analyzed?

By methodically gathering data relating to crucial aspects of cyber-events, the output of this research project will aid in mapping ongoing trends of digital surveillance and address the existing research gap regarding the impact of the spyware market.

III. State of the Art

The objective of this literature review is to take a deeper look at the three main segments of the research: the spyware market, the victims of spyware, and the regulatory frameworks.

(a) Spyware Market

Spyware represents one of the most malicious types of Offensive Cyber Capabilities (OCCs), which, according to Desombre et al. (2021), is the ability to use computer-based tools and techniques to exploit vulnerabilities in computer networks and systems. OCCs are developed and used by different actors, including governments, criminal and private Access-as-a-Service (AaaS) groups that sell computer network intrusion services to clients. Over the years, several AaaS groups have been imitating the private sector and engaging with nation-states to sell their state-of-the-art products and services. These AaaS groups have been proliferating OCCs due to the semi-regulated nature of the market (Desombre et al. 2021).

Considerable academic literature already exists on the definition and functioning of spyware. Moeller (2010) defines spyware as "one type of malicious software (malware) that collects information from a computing system without your consent". Spyware often monitors the activities of users over the Internet and transmits it to an external body (ESCWA 2015). Warkentin et al. (2005) describe spyware as "a client-side software component that monitors the use of client activity and sends the collected data to a remote machine". As Parsons et al. (2017) note, spyware can also act as stalkerware "when surveillance software sold for ostensibly legitimate purposes (e.g., monitoring young children or employees) is repurposed to facilitate intimate partner violence, abuse, or harassment." For the purpose of the study, the research team will be using the definition of spyware as "**a software that is secretly or surreptitiously installed onto an information system to gather information on individuals or organizations without their knowledge; a type of malicious code".**[1] The scope of this project will be restricted to commercial spyware specifically purchased by governments, law enforcement agencies, and private companies at a macro scale for surveillance purposes.

In 2021, the commercial spyware industry was valued at an estimated 12 billion dollars, with an increasing number of governments and law enforcement agencies purchasing these tools (Yung Au 2021). The spyware industry as a whole has become irrepressible as the fall of companies like Germany's FinFisher and Italy's Hacking Team have recently paved the way

[1] This definition is given by the National Institute of Standards and Technology, U.S. Department of Commerce

for newer firms like NSO Group, Cytrox and Candiru to smoothly enter the market as the main sellers of spyware (Feldstein and Kot 2023). **Feldstein and Kot (2023) note that the most unregulated spyware technology used for surveillance originates in Israel, Hungary, Italy, Germany and the United States.**[2]

Several human rights organizations have been actively reporting and documenting instances of spyware as a tool to perpetrate human rights abuses, in particular the violation of the right to privacy of individuals. Civil society organizations (CSOs) are fighting to hold democratic governments accountable for making spyware technologies easily accessible, which are sold to authoritarian regimes that target journalists and dissidents (Woodhams 2021). Woodhams also highlights the need for democratic governments to not only control the supply of spyware products outside their borders but also within their borders (ibid.).

After having accessed the leaked data of 50,000 phone numbers, Forbidden Stories and Amnesty International came together to launch the 'The Pegasus Project', which investigated the NSO Group's Pegasus spyware. The forensic analysis conducted in collaboration with the University of Toronto's Citizen Lab revealed that Pegasus had infected over 180 journalists and several human rights activists, politicians and heads of state from across 50 countries (forbiddenstories.org, n.d.). According to a report by the Citizen Lab (2018), governments in countries such as Bahrain, Kazakhstan, Mexico, Morocco, Saudi Arabia, and the United Arab Emirates have used spyware to monitor and harass political dissidents and human rights activists. In 2016, the United Arab Emirates used Pegasus to target the mobile phone of the prominent human rights activist Ahmed Mansoor, who was subsequently arrested and sentenced to ten years in prison for "insulting the status and prestige of the UAE and its symbols" (OHCHR 2019). In another instance, the Mexican government was accused of using Pegasus to spy on more than 100 individuals, including journalists, human rights lawyers, and opposition politicians (Marczak et al. 2018).

The safety advisory issued by the non-governmental organization (NGO) Committee to Protect Journalists explains how Pegasus has been using cyber-attack features like spear phishing, network injection and zero-click attacks to infiltrate devices. **Once the software has been installed on a device, it has the capability to steal all its data and even convert the infected device into a fully operational mobile surveillance system - all without the awareness or consent of the targeted victim (Earp 2019).**[3] However, there are many more

[2] This observation comes from Feldstein and Kot's extensive database on 'Commercial Spyware and Digital Forensics Technology Procured by Governments' (2023).

[3] The pegasus spyware is capable of accessing phone call records, and messages, discreetly activating the cameras and microphones to capture audio/video-based information (Earp 2019).

products like the NSO Group's Fleming which was marketed as a contact tracing tool during the COVID-19 pandemic but was instead used to breach private data like personal information, health records, and location data (Forensic Architecture 2020)[4]. It is also important to note that there are many other spyware software on the market which have not yet been detected or are harder to find traces of.

(b) Victims of Spyware

Findings from the 'Pegasus Project' show that the targets of the software were overwhelmingly "heads of state, cabinet ministers, diplomats, military security officers, and journalists from the world's top media organizations" (Guterl 2022)[5]. For the sake of the scale of this report, this report will focus on political targets of spyware. There are two main reasons for this specialization. Firstly, while there are several reports on spyware victims for political reasons, based on the current analysis, there is a lack of academic research concerning the harm of spyware from a social science perspective (Schatzberg 2018). Secondly, based on the existing literature, the spyware market seems to proliferate on the large budgets of state agencies and militaries who are able to invest in big purchases and sales (Yung Au 2021). Considering that NSO Group claims to only sell to government intelligence and law enforcement agencies, the interaction between states, spyware and targets can be understood as a political one (Earp 2019b).

Recent reports concerning abusive spyware use by international cybersecurity research institutions are multiplying. Additionally, to the more than 180 potential infiltrations by NSO Group through Pegasus, at least 1,400 users were targeted through WhatsApp (CitizenLab 2020). The list of countries is extensive and any country missing on that list potentially reflects the lack of data rather than the lack of incidents. The targets which have been covered by research reports are often public voices or community leaders who work against the political mainstream, including journalists, activists, NGO workers and religious leaders (Deibert et al. 2022, Al-Maskati et al. 2022, Rueckert & Schilis-Gallego 2020). At the international level, UN Human Rights reports have debated on the dangers of the oppression and abuse perpetrated through weaponization of spyware by state authorities, with a specific mention to its impact on

[4] Another example is the Cytrox's Predator spyware used to attack the devices of Egyptian opposition party politicians (Citizen Lab 2021).
[5] Additionally, non-governmental, humanitarian and international organizations have fallen victim to cyberattacks. One such incident was the large-scale compromise of confidential and personal data of the International Committee of the Red Cross in 2021 (International Committee of the Red Cross 2022).

journalists, human rights activists, lawyers, and political dissidents (OHCHR 2022, OHCHR 2023). Cases such as the targeting of human rights activist Ahmed Mansoor in 2016 and Saudi journalist Jamal Khashoggi in 2018 brought wide attention to the issue of human rights abuse through spyware (Human Rights Watch 2021b, Access Now 2020b). While early findings showed attacks from countries which have low scores on democracy indexes[6], who historically have repressed the right to freedom of expression and political opposition, recent reports show that during the same time frame (between 2015 and 2020) digital surveillance was also conducted in 'democratic' countries who have maintained an image of respecting human rights (e.g., the case of Catalan politicians in Spain, Deibert et al. 2022).

(c) Regulation & Policy

The lack of comprehensive legislative and security frameworks regulating the potential dangers of surveillance technologies has pushed major CSOs and NGOs to collectively advocate for a quicker implementation of enforcement mechanisms and security architectures (Kenyon 2017, Amnesty 2019). The investigations around the supply, demand, and consumption of spyware products, have spurred the development of policies, strategies, and discussions at the national and international level on how to prevent spyware abuses (Human Rights Watch 2021).

While the 2022 study of the EU Parliament on "the use of Pegasus and the existing legal framework in EU Member States" shows that several processes were initiated by EU national governments to criminalize the purchase, selling, and use of spyware, **there is a widespread lack of independent oversight mechanisms and an increasingly low capacity in terms of resources and education on the impact of spyware technologies. Enforcement limitations in existing legislation leave spyware regularization at the discretion of states.**

Khoo (2019) argues on this troublesome aspect by analyzing the EU 2018 General Data Protection Regulation, which legitimizes the lawful use of spyware under certain sets of conditions. These involve when consent of the data owner has been obtained, if control of data is necessary for legal obligations, if conducted by individuals exercising official authorities, or if necessary to protect the life of an individual (Khoo 2019). Criticism by Chan (2018) demonstrates how problematic this becomes when governments themselves are the primary spyware clients and can thus justify their legitimate use in the capacity of official authority. However, the adoption of more specific legislation criminalizing all types of spyware might

[6] Such as the Democracy Index 2022 by the Economist Intelligence Unit

end up being stringent and obsolete due to the continuous evolution of the technological realm (Sipior, 2005). The absence of a categorization and measurement of the degree of harm caused by spyware further problematizes the issue (Wilson 2020). Only through collective efforts of seeking accountability and transparency from national governments can the basic rights and freedoms of people be safeguarded. Also, recognizing the invisibility and subjectivity of potential psychological, social, reputational, political, and economic harms inflicted on the victims is essential to secure their rights of rightful redress and compensation for the abuse suffered.

IV. Methodology

This literature review has been conducted through Open Source Intelligence (OSINT) and desk research in order to accurately reflect the current state of spyware. Documents including research articles and press releases have been retrieved primarily from websites including Human Rights Watch, Amnesty International, The Citizen Lab, The Atlantic Council, AccessNow, Forensic Architecture, Journal of Cybersecurity, and the Committee to Protect Journalists, among others. Policy papers and reports drafted by academic scholars specialized on research around cybersecurity and the digital realm have also been examined. The research criteria entailed the input of keywords and searched queries, such as "spyware", "harm and impact of spyware", "victims targeted by spyware", "Pegasus project", into Google Scholar, JSTOR, and Swisscovery search engines. Qualitative research methodology (Herrera 2004; Birks 2011) was used during the initial phase of research involving the literature review and data collection. However, during the data analysis phase, quantitative research methodology (Birks 2011) was incorporated as well. Grounded Theory (Sosa-Díaz 2022) was adopted as a method of analysis. This allowed the research team to focus on the prior collection and observation of real-life data to then interpret the content and understand the trends and patterns of the phenomena based on the implications of the data analysis. Since real-life data is continuously evolving and spyware is a dynamic phenomenon, grounded theory allowed the research to remain open to the events that emerged during the data collection process (ibid.).

The aim of this research project was to analyze the human and societal impacts of spyware across the world in order to assess the scale of harm caused by spyware. The first phase of the research involved developing a solid database of victims of spyware and the associated harms and events through the systematic collection of data over the past ten years (2013-2023) using OSINT research. This preliminary research phase entailed a categorization of the potential targets of spyware, clients of the spyware industry, the tools used by perpetrators to inflict harm, and the impact of the event(s) on the victims. The data was collected by scanning media reports, news articles, research papers, academic and scholarly journals, reports published by NGOs, governments, and International Organizations (IOs).

The data analysis phase was split into two sections: quantitative analysis and qualitative analysis. For the quantitative section, the team used Microsoft excel tools to analyze the data and identify any emerging patterns and relations. The analysis was conducted through categorizing the data into broader notions of "events", "targets", "event-targets" and "sources". In the qualitative findings section, the research team worked on creating a matrix for assessing

the harm caused by spyware across actors, events and tools (Figure 13). The findings that emerged during the data collection process were interpreted using a content analysis research method, which allowed to identify the presence of certain concepts and themes within the qualitative data (Herrera 2004). For the content analysis a 'semi-open-code' approach was used which allowed both for the analysis of the data based on the harm assessments mentioned in the literature (Agrafiotis et al. 2018; Korff 2020; Richards 2013; Ignatuschtschenko 2021), as well as for the identification of mentions of harm that are conceptually outside of these frameworks to incorporate them into the analysis based on an 'open code' methodology (Agrafiotis et al. 2018). The iterative process of the 'open code' approach allowed for the creation of themes based on the repetition of identical concepts within the data. As part of this research phase, three case studies, chosen based on the findings from the data collection, were further discussed. **Overall, the consolidation of qualitative and quantitative research methods, OSINT research, and the categorization of targets, tools and harms helped to engage with the research questions posed by the project.**

While such methodology allowed for a deeper understanding of the current spyware market, it is not without limitations, risks, and constraints. A fundamental limitation concerned the harm assessment, as there is currently no clear index or scale for comparing and quantifying the type of cyber harm suffered by the targeted victims. Attempting to identify such indicators might have led to dangerous misrepresentations of subjective degrees of harm that often depend on the single individual. The research project also confronted itself with the distinction of the consequences deriving from spyware abuse, including risks, impact, and human rights violations. Differentiating between these terms was necessary to avoid trivialization.

Within research harm and impact are used as interchangeable terms concerning the negative consequences of illegal spyware use. Agrafiotis et al. (2018) elaborate on these terms and state that while 'harm' is used to describe negative outcomes of the interaction between individuals and the cyberspace, 'impact' is commonly used for consequences of any nature (good, bad or neutral). However, the discourse around surveillance and security shows that impact is often used to refer to negative consequences (3). Thus, these terms were used interchangeably for the purpose of the research. Risks refer to the likelihood of a threat being carried out (United Nations Security Management System 2017). Human rights, according to the UN Human Rights Office of the High Commissioner, are "rights we have simply because we exist as human beings". The failure to respect, protect, or fulfill any of the human rights set out under the Universal Declaration of Human Rights constitutes a violation of these (OHCHR).

A second aspect to consider concerned the risk of generalization that might have arisen from the output of the data. The categorization of the targets was carried out based on the demographic data that emerged from the preliminary data collection and analysis. Targets were categorized based on their gender, religion, ethnicity, nationality, and profession. To minimize the ethical risk, the research team was sensitive to the fact that targets might possess intersectional identities which might overlap and exacerbate any potential harm, as well as that there were certain limitations in ascribing categories to people without the necessary information publicly available. Moreover, experiences related to spyware abuse were likely to differ depending on sociocultural context, technological capabilities, and targeted individuals. Generalizing patterns of cyberattacks and their impact and harm on individuals might become troublesome for future literature.

V. Preliminary Research and Findings

(a) Quantitative Findings

The research team used Microsoft excel tools for conducting a thorough analysis of the data collected in the preliminary research stage. The key observations of the data analysis stage will be discussed below. For the purpose of the analysis, data was divided into four key sections: Events, Targets, Event-Targets[7] (links between targets and events) and Sources.

(i) Events

The research team defines an "Event" as a spyware attack that was instigated against the targets (whether successful or not). **A total of 53 events over the course of 10 years starting from 2013 to 2023 were identified.** As Figure 1 demonstrates, the number of events has risen nine times from 2013 to 2021 with some fluctuations over the period of time.

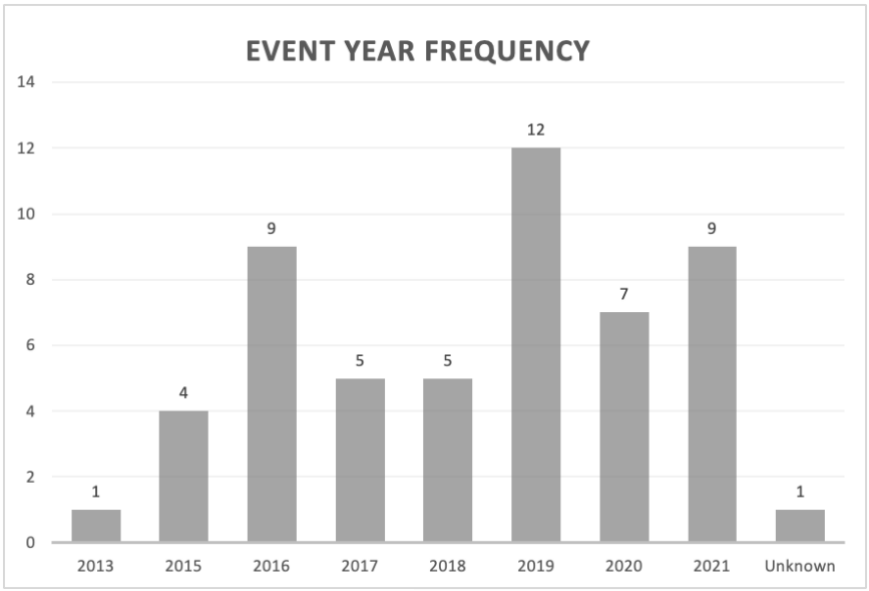


Figure 1: Event Year Frequency

Out of these 53 events, 20 involved single targets and 33 affected multiple targets. The data identifies 12 regions around the world where these events occurred[8]. **The highest number of events were observed in the regions of Central America, Western Asia, and Western and Southern Europe.**

[7] Complete data sheet can be found in Annex I.
[8] The regions were defined based on the system of the United Nations Statistics Division.

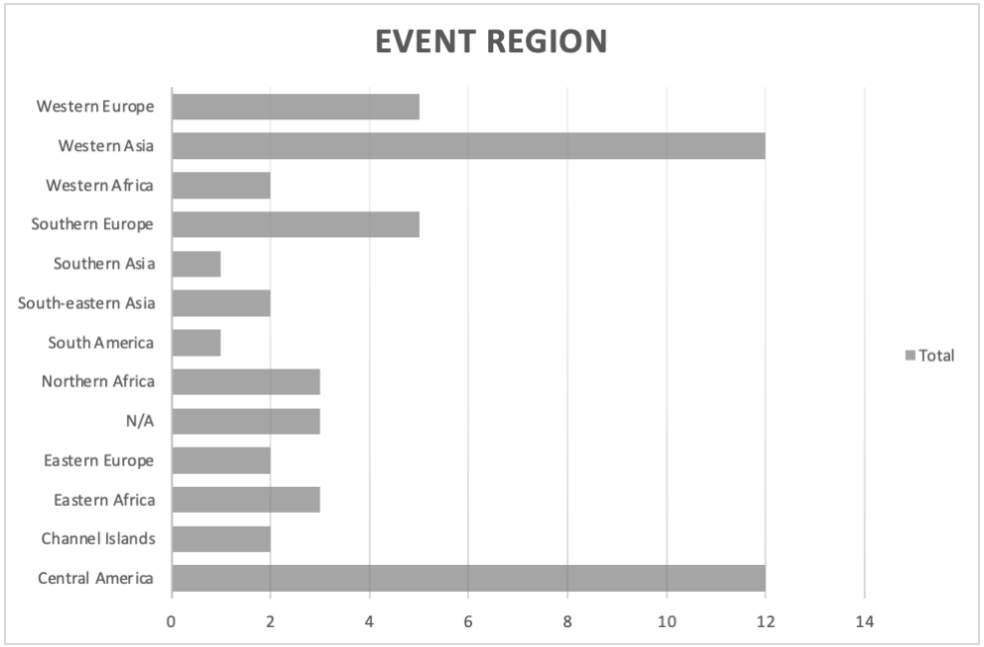


Figure 2: Region Event

Mexico recorded 11 events which is the highest number of events documented over the period of analysis. **Most of the spyware attacks were found to be launched by NSO Group's Pegasus spyware.** Pegasus was responsible for about 42 events, followed by Cytrox's Predator that initiated two events. Some other spyware software that have been used are Finspy, Hacking Team's Remote Control System, Karma, Invisible Man, PC surveillance system, Kerrdown, and Exodus. **The data confirms that governments constituted the highest percentage of customers of spyware (57 percent) followed by unknown customers and Intelligence agencies.**

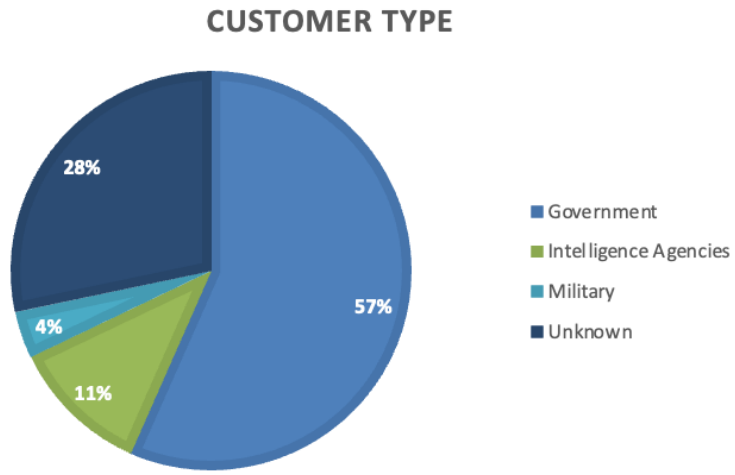


Figure 3: Customer Type

Finally, the research showed that only 24 percent of the total events were transnational in nature, whereas 70 per cent of the events happened within the domestic territories of the countries. In terms of the regions, Western Europe was found to have the highest number of transnational events.

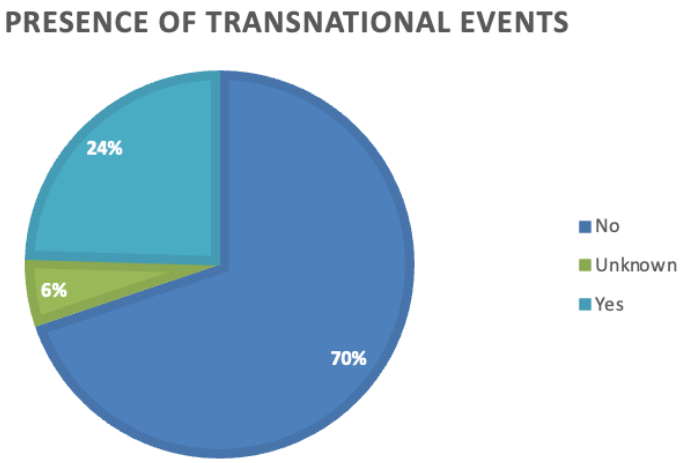


Figure 4: Presence of Transnational Events

(ii) Targets

"Targets" are defined as journalists, human rights defenders, NGOs, politicians and/or individuals whose profile is not of a criminal or terrorist nature. **The research team identified and collected information on the demographic characteristics of 216 targets in total, including 34 unknown targets.** The greatest number of targets belong to El Salvador, followed by Spain and Thailand (Figure 5). The total number of targets is however not indicative of the number of events taking place in a country. For example, the large number of targets in El Salvador were part of a single event that took place between July 2020 and November 2021. The phones of 35 Salvadorian journalists and civil society members were infected with Pegasus while they reported on sensitive issues related to the government, including the negotiation of a "pact" with the MS-13 gang which enabled the increased infiltration of gangs in private security firms (Scott-Railton 2022b).

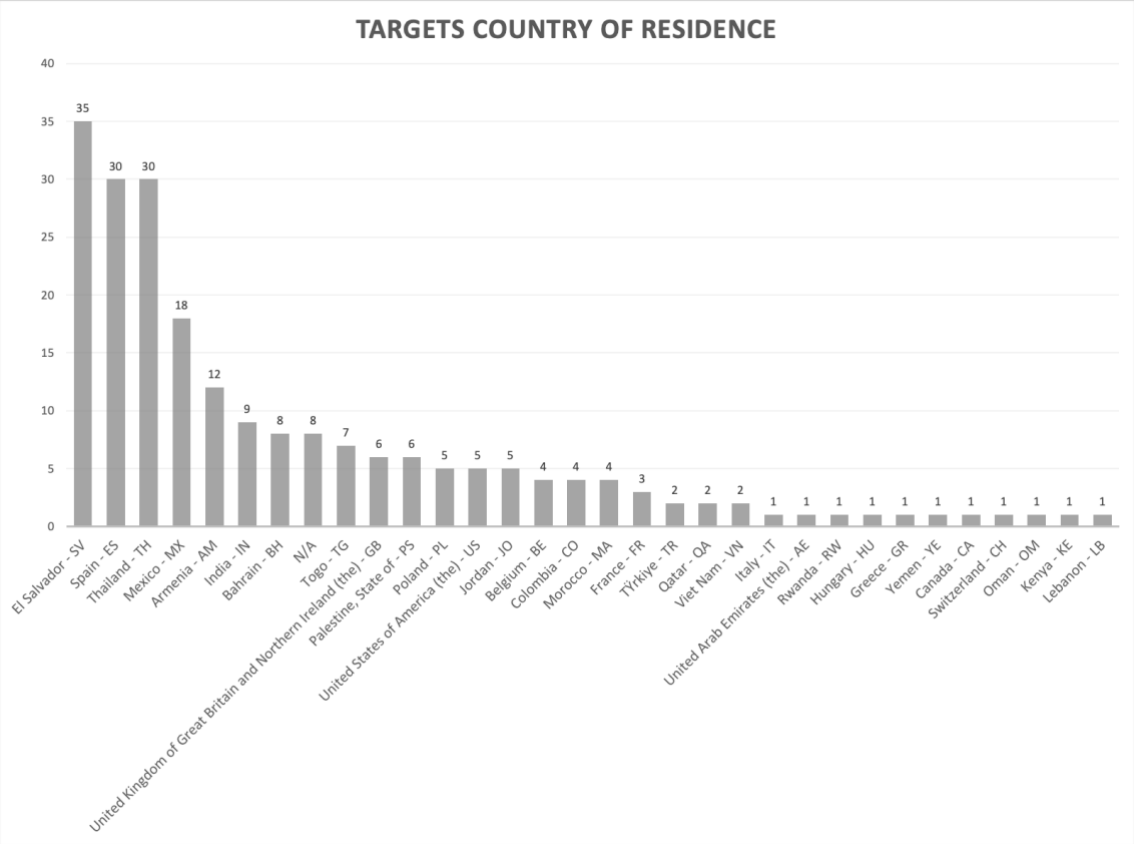


Figure 5: Targets Country of Residence

Over 80 percent of targets belong to the sectors of Advocacy, Media and Politics with Advocacy being the most targeted sector (Figure 6). The least number of targets belonged to the sectors of "Humanitarian" and "Community-Spiritual and Faith based" (One percent each). Within Advocacy, activists were the prime targets with most targets from Thailand. These targets represent at least 30 pro-democracy activists who were calling for reforms to the monarchy with mass protests and social media campaigns, while they were targeted in Thailand between October 2020 and November 2021 (Scott-Railton 2022a). The spyware infections were preceded and succeeded by arrests and detentions, and activists were harassed and threatened both online and offline, even outside the country (ibid)[9]. In the sector of Media, investigative journalists were prime targets, with most from El Salvador. In Politics, political activists were the main targets, with most of them from Spain. About 87 percent of the total targets were Individuals whereas 6 percent were political parties and organizations.

[9] The Thai government allegedly acquired surveillance technologies from Hacking Team in 2013 and 2015, and subsequent research by the Citizen Lab suggests that they also acquired a complementary program to Pegasus to intercept phone calls, SMS, and track phone locations without hacking the devices (Scott-Railton 2022a).

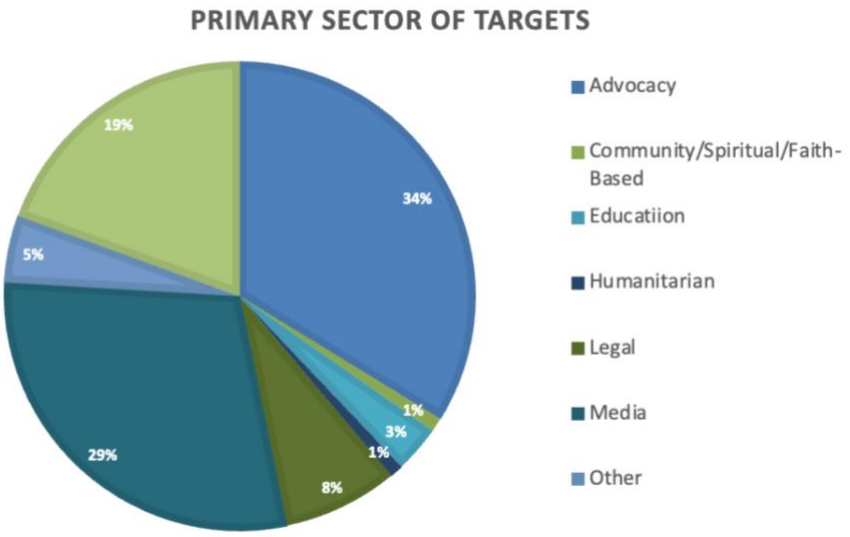


Figure 6: Primary Sector of Targets

In terms of the gender of the targets, 53 percent were males, whereas 25 percent were females. The research team, nevertheless, was unable to find the gender of all the targets. Hence, some were labeled as "unknown". As some targets were part of political groups and organizations, the label "N/A"" was used. There were more male targets with Black, South Asian, Hispanic, White, and Middle Eastern ethnic backgrounds, whereas, there were more female targets with Asian and Mixed ethnic backgrounds[10].

As not much personal information of the targets was available, most of the targets' religion was deemed "unknown". However, Muslim targets were found to be higher than Hindu, Christian, and Buddhist targets.

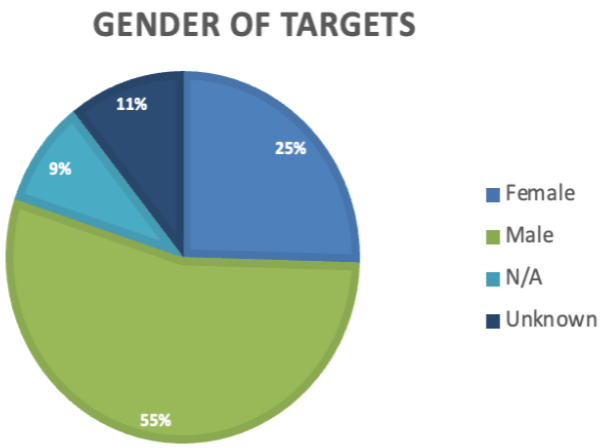


Figure 7: Gender of Targets

[10] A deeper analysis of the specific cyber-events would be interesting in order to make sense of the gender gap, especially considering the harm inflicted by malware discussed in the next chapter.

(iii) Event-Targets

The research team defines "Event-Target" as the overall impact on targets linked to the individual events involving the usage of spyware products and the types of attack vectors. **The highest number of targets (including unknown targets) were linked with the event in Spain (Catalonia)**, where 65 individuals from several civil society groups were targeted and infected with spyware (further discussed in Chapter VI). Subsequently, 12 targets were linked with the event in Armenia, where several Armenian journalists and human rights defenders were targeted with spyware.

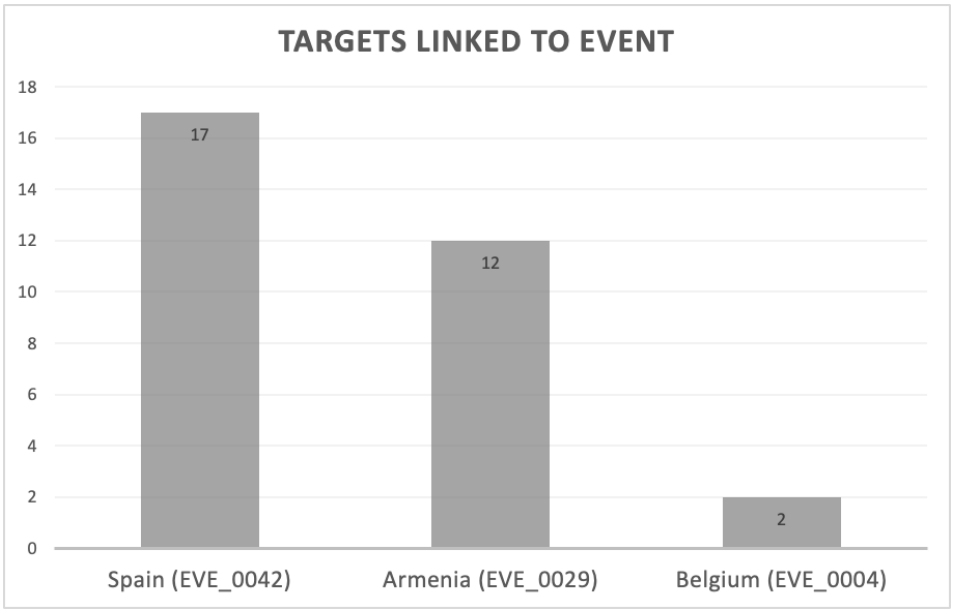


Figure 8: Targets linked to Event

Zero-Click Exploit was found to be the most common form of attack vector with about 55 percent of the event-targets being attacked by it.[11] It is interesting to note that 70 percent of the targets working in the Advocacy sector and 63 percent of the targets working in the Media sector were mostly attacked by the invisible zero-click exploit, which shows their peculiar vulnerability to spyware surveillance. Most targets in the Humanitarian and Politics sector were attacked by unknown vectors. The Education, Legal, and Community-Spiritual and Faith based sectors' targets were attacked by phishing, which involves receiving messages with deceiving

[11] A zero-click exploit is a malicious malware that can be installed on a device without the victim's knowledge. Unlike other spyware exploits, it does not require the victim to click on any link or message, hence it is considered highly dangerous (Kaspersky 2023).

information on one's devices, designed to make targets click on links, pictures or documents which will lead to an infiltration.

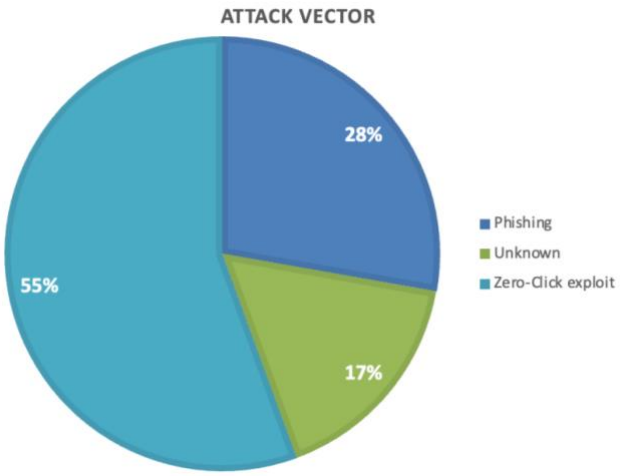


Figure 9: Attack Vector

(iv) Sources

For the purpose of research, the team scanned through a total of 62 sources, out of which 43 percent were derived from non-cyber-centric news outlets and 39 percent were from Academic/Research Institutions/Organizations. Most sources were derived from reports published by the Citizen Lab and news articles published by The Guardian.

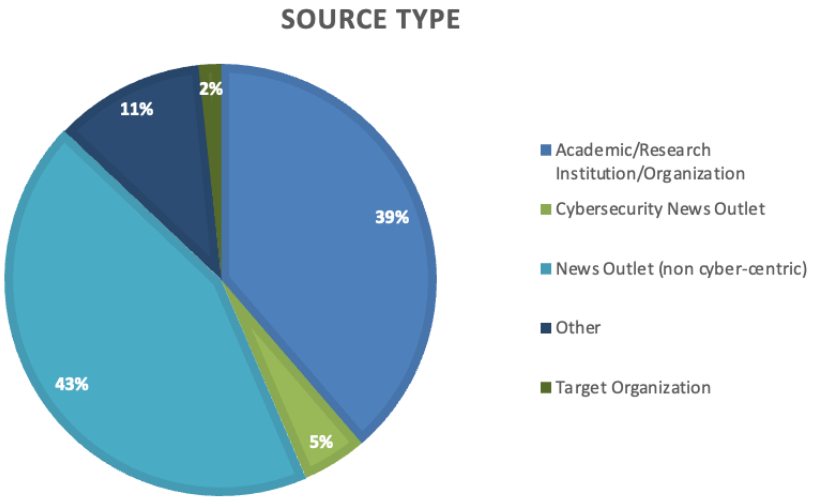


Figure 10: Source Type

(b) Qualitative Analysis

The collected data allowed for the identification of common patterns of victims' experiences of harm in order to describe the impact of spyware attacks. The greatest challenge in the analysis and elaboration of a cyber harm grid is the lack of existing, agreed-upon definitions of cyber harm in the academic literature. Agrafiotis et al. (2016) attempted to fill the gap by defining cyber harm as the negative outcome arising from intentional or incidental cyber-events within or beyond the boundaries of the internet (2). They later added that cyber harm may also be understood as the infringement of the 'welfare interests' of individuals, as those basic needs for people to function as "purposeful, self-reflective and responsible agents" (2018: 3). Similarly, Bellaby (2012) described the harm caused by intelligence collections as the impairment of the most important requirements for the well-being of individuals, such as autonomy, liberty, mental and physical integrity, privacy and human dignity (95).

These considerations are especially important, considering that spyware harm might often not be felt on a physical level, yet people can still be harmed if their intrinsically welfare interests are violated (96). Additionally, if cyber harm is considered to be the violation of the most fundamental 'primary goods' of humanity, they may also be considered to be global forms of harm. As Bellaby (2012) states, while it is important to remain skeptical of any 'universal' notion of the human experience, harm can still be measured along the vital interests common to all people (97), such as mental and physical integrity and human dignity. **Based on the existing literature, the research team defines cyber harm as the damaging consequences resulting from cyber-events affecting individuals' welfare interests, including the target's digital devices, physical and psychological integrity, financial security and social or political standing**.

The literature and research also identified several challenges which remain in the preliminary framework of the harm assessment. First, as mentioned in the methodology section, the quantification of harm is problematic considering that effects and severity are subjective and based on different individual variables, including age, gender, experience, cultural and societal norms, and natural disposition. For a credible evaluation, it is important to note that the impact may differentiate based on whether the harmed subject is an individual or an organization, which category the harm experienced falls into, and which factors are considered while measuring harm (Agrafiotis 2016). The intangibility that characterizes cyber harm requires a harm assessment that allows for a deeper analysis case by case. **In this respect, this research project can represent a starting point for the development of a methodology**

measuring harm from both a quantitative and qualitative perspective. Based on the literature review and the results from the open analysis of the research data, the following matrix of harm was used to code, categorize and analyze the harm caused by spyware use (Figure 11).

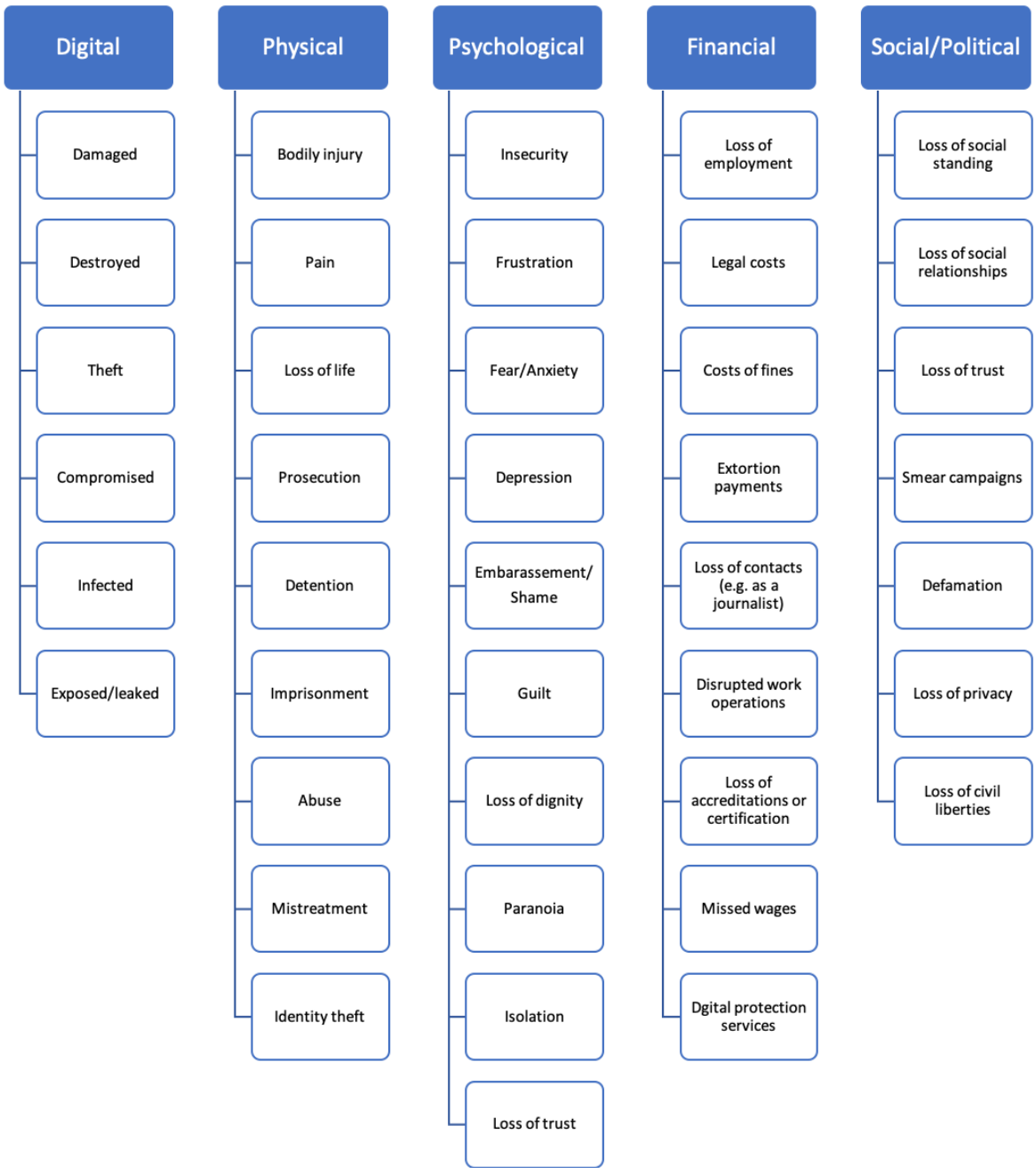


Figure 11: A matrix of cyber harms

(i) Findings

A preliminary analysis of the data shows that of the recorded 216 targets who experienced a spyware event, 164 experienced an infection of their digital devices[12]. Thus, out of all the categories, the digital harm category is - understandably - the most prominent one. 20 targets experienced social or political harm, which often related to smear campaigns or loss of privacy or civil liberties[13]. 17 targets experienced severe psychological harm, most notably fear, anxiety, insecurity, a feeling of paranoia[14], loss of trust, and isolation. Eight targets suffered physical harm often relating to the prosecution, detention and imprisonment of targets. Some of these harmful experiences around spyware attacks can only circumstantially be attributed to the event itself, but might nonetheless be important to mention. For example, an extreme case of physical harm was experienced by the blogger Yusuf Al-Jamri, who was tortured by the Bahraini Intelligence Agency in 2017 before seeking asylum in the UK in 2018 (Marzack et al. 2022). His device was infected with Pegasus either before or after being tortured (ibid.). Thus, the torture or the spyware infection can be seen as a consequence of the respective other, but in any case, they seem to be intercorrelated.

Only six targets mentioned financial harm in direct relation to the spyware incident. These six targets work in professions that were made increasingly difficult through the spyware abuse, such as journalists, lawyers, priests and Human Rights Defenders (e.g., journalists that are no longer able to be in contact with sources through digital devices). One of those targets was Aida Alami, a Moroccan journalist, who was spied on through the Pegasus software most probably by the Moroccan state. She stated in an interview that the cyber-event has made her job much harder, as sources are scared to talk to her in fear of potential retaliations (Guterl 2022).

An erosion of trust in the digital realm through a cyber-event often leads to skepticism and lack of confidence, undermining active engagement with technological devices and services. The collected cases of spyware abuse showed that these feelings were widely shared by the targets. In one instance, the victims claimed to "have been living in a state of daily anxiety and fear since they discovered their phones were infected" (Frontline

[12] While all 216 victims experienced a targeting (including receiving suspicious emails, messages or phone calls) not all targets were successfully infected with spyware. For some, there might also be a lack of evidence of an infection which implies a larger dark figure for targets who were infected.

[13] Even though all targets experienced some form of privacy and civil liberty loss, these targets were marked for this category either for the severe experience thereof or because it was explicitly mentioned in interviews.

[14] Although paranoia is a concept in psychology, the term used here is understood to be separate from the medical definition. 'Paranoia' is used as a self-descriptor of the people recorded in the data set, and often refers to the feelings that are provoked when people fear the penetrating and all encompassing surveillance enacted by states or state agencies.

Defenders 2022). In other spyware abuses, victims shared a sense of insecurity when using their phones, claiming that the surveillance abuse "gives a very dirty feeling" where "personal privacy gets rudely violated" (The Wire Staff 2021; Krapiva 2023). Spyware victims also described the spyware attacks as having a "huge psychological impact" and as "extremely traumatic", comparing it to "torture" when "thinking about all your private life, personal problems in the hands of strangers" (Rozen 2021). Echoing these common feelings and perceptions, a target also claimed to be "in a state of paranoia, anxiety, and terror" after learning that their personal information had been compromised, affecting both their professional and personal life due to fear of endangering acquaintances or others' fear of getting in contact with them (Frontline Defenders 2022).

Other cases strongly expressed their harm in human rights terms. **Victims emphasized the violation of their right to privacy, feeling insecure in their movements and their surroundings** (Al Jazeera Staff 2021; Abu Sneineh 2021; Citizen Lab 2021; Frontline Defenders 2022). A victim referred to her spyware attack as having compromised her right to dignity, leading to a loss of her "space to express" (ibid.). This infringement on the right to freedom of expression and opinion is also visible in other instances, where targeted victims' phones were infected with spyware, exposing sensitive information contained in the phone's contacts, emails, messages, and camera (Scott-Railton 2017; Noguera 2020; Sabbagh 2021). Human rights campaigner, David Haigh, claimed that the attack amounted to "state-sponsored harassment" (Sabbagh 2021).

Another interesting assessment of harm shows the long-lasting and widespread harmful effect abusive spyware has on the communities of the spyware targets. The curtailing of freedom of expression and the shrinking of civic space through the spread of fear of state surveillance not only affects the target itself, but often also the surrounding social circles of the spyware victims. The data shows that the targets experience insecurity towards future surveillance, and feelings of shame and guilt towards the people in their surroundings who might have been exposed to surveillance because of them (Fakih 2022, Guterl 2022, Fouriezos 2022). When journalists, lawyers, human rights defenders and other important figures in society are surveilled and harmed, not only does this impact their sources, contacts, clients and families but also the people who might profit from their work.

For example, Julia Gavarette, a Salvadoran journalist who was infected with NSO's Pegasus 18 times in 2021, explains the long-lasting effect the surveillance has had on her work: "This is one of the *most significant pressures* that I have had to deal with. I was cautious before, but [now] I am even more extreme to avoid putting sources in danger. But *it wears you out*

day-to-day, and you have to make an even greater effort to be able to produce journalism" [emphasis added by author] (Earp 2022). Another example is Ghassan Halaika, a HRD working for a human rights organization in Palestine (Al Jazeera 2021). He was surveilled in 2020 and stated in an interview with Al Jazeera how devastating the impact of the spying was on his work: "What really hurts is that confidential information I had worked on with private contacts, in regard to pursuing Israeli war crimes at the International Criminal Court, was uncovered during the surveillance and has hurt some of my contacts" (ibid.).

Moreover, despite the research showing that a minority of the spyware targets are female (25%), both Access Now and Front Line Defenders report that women who have been targeted by spyware are especially impacted and that their harm is particularly severe (Fatafta 2022). One example is the case of the Bahraini human rights defender Ebtisam Al-Saegh, who, after having been targeted multiple times in 2019 by spyware linked to NSO Group, started to change her behavior drastically because of constant anxiety for further retribution and exposure (ibid.). Access Now noted that Al-Saegh started to wear her veil even when she was alone in her own home, out of fear that she was being watched (ibid.).

As the data collection of the impact description was not structured (open comment), the findings might potentially be skewed in any one direction. During the process, the research team noticed that the initial accords of the spyware events often only carried information about the digital infections. There were hardly any accounts on the subsequent harm experienced by the targets[15]. Such accounts were often only found in newspaper articles with interviews or personal statements by the targets. This implies that the data collected potentially lacks records of a large portion of the harm experienced by targets. For future research, it will be important to review the findings and to add information where available and necessary. Finally, a deeper analysis on the basis of three case studies, each of which entails singular importance to the data collection, will help to exemplify and contextualize the harm experienced by people on a grander scale.

[15] This could also be due to the fact that some targets were anonymous and some spyware incidents involved more than twenty targets, making it difficult to provide a detailed account of each target.

VI. Case Studies

To exemplify the issue of spyware and its impact on people, the research team selected the following cases: (a) A specific case of spyware abuse against Catalan politicians in Spain and Europe; (b) An assemblage of cases crossing borders in Western Asia targeting journalists and human rights defenders; and (c) The abundant use of spyware against multiple targets in Mexico. **The research data showed that these three places (Spain, West Asia and Mexico) belong to the top four regions with the highest number of events recorded.** These three case studies deal with targets such as **human rights defenders, journalists, and opposition politicians, who belong to the top three primary sectors that were targeted with spyware (Advocacy, Media, Politics).** The cases further help to comparatively illustrate the harm caused by spyware to individual targets, as well as the broader harm inflicted to the communities at large.

(a) Case Study 1: Spyware abuse against supporters of Catalonia's independence

The first case examines the spyware abuse conducted against Catalan politicians and political activists with the aim to silence opposition and dissent. This case represents only one of the many cases of spyware abuse against political figures and human rights activists engaged in the push for governmental change. Agrafiotis et al. (2016) refer to the risk of political/governmental harm as encompassing "the disruption of political processes, which may include, among others, the electoral system, the policy-making process, citizen engagement in political processes and the criminal justice system". The Catalan case represents a significant instance of the combination of Agrafiotis' political harm with Ignatuschtschenko's (2021) concept of erosion of trust. The Catalan spyware attack consisted of a widespread infiltration of Pegasus and Candiru spyware software against, as reported by CitizenLab's report (2022), at least 65 individuals from the Catalan government, civil society organizations, NGOs, European Parliament members, lawyers, and human rights activists. In some cases, even close acquaintances and family members were targeted or infected. While the exact perpetrator of these attacks remains unconfirmed, substantial evidence points to the involvement of the Spanish government's National Intelligence Center (CNI) (Citizen Lab 2022). Pressing demands from the United Nations and the European Union to investigate into the alleged

Spanish spying program inflicted considerable reputational damage on the government itself, diminishing public confidence in the Spanish democratic credentials of respect for fundamental human rights values (Jones 2022).

Spain and Catalonia have a long-standing history of conflict stemming from Catalonia's declarations of self-determination and Spanish courts' rulings of the Catalan secession desires as a violation of Spanish constitutional law. In 2014, the dispute escalated in a two-year ban of former Catalan president Artur Mas from holding public office after leading a non-binding symbolic referendum on self-determination (Jones 2017). A second turning point was in 2017, when Carles Puigdemont, Mas' successor, announced a binding independence referendum, defying the Constitutional Court ruling. The Spanish government promptly suppressed the movement by dissolving the Catalan parliament and denouncing Carles Puigdemont, President of Catalonia at the time, for rebellion (BBC 2019; Citizen Lab 2022). These 2015-2020 Catalan pro-independence political tensions were the background for the extensive spyware attacks against Spanish dissidents and supporters of the Catalan secession.

Victims discovered the targeting in 2020 as WhatsApp and Citizen Lab notified them of their phone's infection during the WhatsApp Pegasus breach in April 2019, when 1,400 users were reportedly targeted through a zero-click vulnerability exploited by the NSO Group (Kirchgaessner 2020). Among the prominent victims were pro-independence president of the Catalan parliament, Roger Torrent, the leader of the Republican Left of Catalonia party, Ernest Maragall, the former regional parliamentarian of the far-left party, Anna Gabriel, human rights activist Jordi Domingo and Puigdemont's collaborator, Sergi Miquel Gutiérrez. A common factor among all victims was that the Pegasus infections occurred during crucial political debates and negotiations between the Catalan and Spanish governments (Citizen Lab 2022).

Concerning members of Catalan civil society organizations such as the Òmnium Cultural and the Assemblea Nacional Catalana (ANC), their online surveillance resulted in arrests and imprisonments. An example is ANC president Jordi Sànchez, who was targeted in April 2017, when the Catalan government met with civil society groups to discuss Puigdemont's referendum. The Pegasus surveillance that occurred in the next months ultimately led to Sànchez's arrest due to his involvement in the illegitimate referendum. Similarly, Citizen Lab's analysis (2022) found that journalist Meritxell Bonet, wife of former Òmnium president Jordi Cuixart, was under surveillance while Cuixart was being prosecuted for his role in the 2017 referendum.

The occurrence of the exclusive targeting exclusively of independence supporters during important political calamities strongly suggest that the surveillance intended to disrupt Catalan autonomy efforts. This close monitoring was coupled with a violent offline repression of political dissent. The Spanish government's suppression of protests, and persecution, imprisonment, and forced exile of pro-independence activists and political figures represented a severe threat to democratic governance and values (BBC 2019). Meritxell Serret, Minister for Foreign Action and the European Union, expressed her concerns about the spyware abuse as an "unprecedented attack on a democratic movement as a whole" carried out by a democratic government itself and a member of the European Union (Tar 2023).

As collective calls for investigation and adoption of tighter surveillance regulations rise, current Catalan president Pere Aragonès, also a victim of the Pegasus attack, recently claimed, in April 2022, how the targeting of his phone "goes beyond what has been done to [him] as an individual and as a citizen. They also attacked the democratically elected institution that is the Catalan government, which is an attack on all Catalan citizens and institutions, and as such an attack on democracy" (Jones 2022).

(b) Case Study 2: The Struggle for Privacy and Freedom of Expression in Western Asia

A second case study examines the loss of the right to privacy and freedom of expression of human rights defenders, journalists and civil society activists in Western Asia. The area has been observing continuous cyberconflicts between different groups, delineated by regional rivalries, political alliances, and sectarian divisions (Al-Rawi 2019).

The targeting of over 36 Al Jazeera and Al Araby TV journalists between 2019 and 2020 by NSO Group's Pegasus spyware was a multifaceted event involving several actors (Marczak et al. 2020). As per the Citizen Lab report (2020), the attacks were attributed to the Pegasus operatives MONARCHY, deployed by the Saudi Arabia government, and SNEAKY KESTREL, deployed by the UAE government. Out of the 36 media personnel, only two investigative journalists consented to be identified during Citizen Lab's investigations. Tamer Almisshal, a Palestinian investigative journalist working with Al Jazeera had covered the stories of members of the UAE royal family and journalist Jamal Khashoggi's assassination, and Rania Dridi, a Tunisian TV news anchor who hosts shows on Qatar's Al Araby TV

covering politically sensitive topics related to women's rights issues (Kirchgaessner and Safi 2020).

The media network of Al Jazeera is based in Doha and is funded by Qatar (About Us. Today's latest from Al Jazeera, n.d.). Although its presence has been known for influencing opinions in the Arab world, it has been accused of biased reporting towards the state of Qatar, which has affected Qatar's diplomatic relations with other countries of the region (Al-Rawi 2017). In 2017, Saudi Arabia, Bahrain, Egypt and the UAE suspended diplomatic ties with Qatar as Qatar's Emir was falsely quoted by the Qatar News Agency (QNA) for commending Iran, Saudi Arabia's prime adversary (Marczak et al. 2020). Later on, it was observed that this disinformation campaign was a result of QNA's hacking, which was attributed to UAE authorities (DeYoung and Nakashima 2017).

Jones (2023) talks about how novel digital monitoring methods such as spyware surveillance have been playing a vital role for emerging digital authoritarian coalitions within the region. Countries like Israel have been actively involved in selling invasive surveillance technologies to Saudi Arabia, the UAE, Morocco, Jordan, Bahrain, etc., who have been using these spyware tools not only against dissidents and activists of their own countries but also against those residing abroad (Jones 2023). The Access Now report (2023) further discussed the deployment of Pegasus in the Azerbaijan-Armenia conflict. Armenian spyware victims were found to have sensitive information regarding the Nagorno-Karabakh war on their mobile devices. This raised concerns regarding privacy, cyber warfare, and potential violations of human rights as digital espionage tactics were used by both sides to suppress dissent of political groups, civil society members and journalists (Access Now 2023).

In Jordan and Bahrain, spyware surveillance has had a damaging impact on Women Human Rights Defenders' (WHRDs) right to privacy and autonomy (Unsafe Anywhere 2022). After being targeted by Pegasus, Hala Ahed Deeb, a Jordanian Human Rights lawyer expressed: "When your privacy is violated, you feel violated, naked, and with no dignity— this is how I feel" (Unsafe Anywhere 2022). She expressed her fears of being a woman and losing her privacy and space to express in a conservative society. She felt isolated and started practicing a form of self-censorship to avoid communicating with people around her. This resulted in her experiencing a form of paranoia as she felt that she was constantly being surveilled. Such violations of privacy were also claimed by Ebtisam El-Saegh, a Bahraini human rights defender, who was put in a perpetual state of "fear and terror" when her phone was hacked eight times by Pegasus in 2019 (Unsafe Anywhere 2022). The spyware attack also made her experience paranoia, thus terribly affecting her personal and professional life, and

disrupting her relations with people. In a report by Front Line Defenders (2022) she exclaimed: "Personal freedoms are over for me, they no longer exist. I am not safe at home, on the street, or anywhere."

(c) Case Study 3: The erosion of accountability through spyware in Mexico

The third case deals with the abundant and illegal use of spyware in Mexico, which, according to the research findings, has recorded the majority of such cases. This is indicative of a trend, as for example a third of the 50,000 numbers leaked as potential Pegasus targets by Forbidden Stories were also from Mexico (Pieper 2021), with journalists, digital rights groups, and HRDs and their families representing the majority of these targets (Southwick and Martínez de la Serna 2022). This is especially worrisome, considering that Mexico has been declared to be the deadliest country for journalists in the world for four consecutive years since 2019 (Reporters Without Borders 2022). While the government pledged to stop their involvement with illegal surveillance tools in 2018, the numbers of targeted and infected devices of Mexican journalists and HRDs continue to rise (Hootsen 2022).

To date, the already few laws protecting people from falling victim to the intrusive and unethical use of spyware in Mexico are poorly respected (ibid.). Furthermore, according to a report by Proceso, the Mexican government paid 16 million US dollars in October 2021 to a person who was responsible for the purchase of Pegasus (Tourliere 2021)[16]. Developments in Mexico also show that many cases of spyware programs may have involved non-state actors and that a number of infections and targeting of journalists happened while they were working on investigative pieces concerning cartels (Hootsen 2022.).

While the research team collected 26 targets overall in Mexico (including other professions which were not mentioned above), a report by Forbidden Stories shows that at least 25 targets of spyware in Mexico alone were journalists (forbiddenstories.org). One such case involved the spyware infection of the devices of Javier Valdez' wife and coworkers after he was shot twelve times in May 2017 in front of his office (Red en Defensa de los Derechos Digitales 2018). Valdez was a prominent investigative journalist who worked intensively to uncover organized crime and cartels in Mexico. His work on the rising tension in the wake of

[16] This is after the government had already spent $61 million on NSO Group spyware from 2006 to 2012 (Associated Press, 2021).

the arrest of the Sinaloa cartel boss 'El Chapo' was what led to his murder, which was internationally considered a cartel killing (Scott-Railton et al. 2019; BBC News 2018; Esquire 2018).

Two days after his death, Andrés Villarreal, a journalist and close colleague of Valdez, received a notification on his phone, prompting Villarreal to click on a link enclosed in the message (Scott-Railton et al. 2019). The link led to a website called animal-politico(.)com, which was a domain claiming to be the official Animal Político outlet and was previously identified to be part of the Pegasus infrastructure in Mexico by a Citizen Lab report (Scott-Railton et al. 2019). Between 17 and 26 May at least six such messages with links to the Pegasus malware were sent to Andrés Villarreal and another journalist close to Valdez, Ismael Bojórquez (ibid.). Griselda Triana, Valdez' wife and a journalist as well, was also targeted multiple times with the same spyware ten days after he died (Scott-Railton et al. 2019). She similarly received messages prompting her to click on an exploit link which would have led to an infection with Pegasus. The messages were sophisticatedly designed and referred to the ongoing investigation of her husband's murder in order to prompt her to click on the malicious links (ibid.). Luckily, Triana recognized the strange content and timing of the messages and forwarded them to the human rights organization Article 19, who, together with SocialTic, R3D and Citizen Lab started to investigate the origin of the spying attempts (ibid.). Triana later questioned the absurdity of using state sponsored spyware on her: "What reasons were there to spy on me? Neither I nor my family are criminals, and I am sure that I do not represent any danger to national security" (Verza 2019).

While the journalists and Triana never got confirmation on who the perpetrator was, the case seemed clear for Villarreal, when he stated: "The spyware is just a new aspect of a problem that has always existed. The authorities have spied here, they will continue to do so" (Hootsen 2022). In Mexico, the use of spyware appears to be part of a greater problem of increasing subjugation and violence used against journalists, and on a greater scale the Mexican population, not only by the state but also by criminal organizations such as the cartels (Southwick and Martínez de la Serna 2022). Additionally, Pegasus is just one of many spyware tools used and applied by the Mexican government. R3D has warned that there are multiple other technologies which were recently acquired by the state (ibid.). As Scott-Railton et al. state: "The repeated use of Pegasus to target journalists and their family members over multiple years suggests a pattern of official abuse" (2019).

VII. Insights and Conclusion: Discussion with the Case Studies

The case studies examined above specifically shed light on how spyware abuse was directed towards individuals and groups engaged in dissent. Dissent, defined as expressing disagreement with politically or socially regulated issues, plays a crucial role in promoting progressive social change and communicating opposition to the status quo (Perlman 2019; Zick 2019). The case studies predominantly involved human rights defenders, journalists, and opposition politicians who engaged in political dissent. These individuals were targeted by governments in Spain, Saudi Arabia, UAE, and Mexico, which utilized spyware as repressive surveillance tools. According to Ritter and Conrad (2016), repression and dissent are intertwined, as governments employ repressive tactics to suppress dissenting activities, leading to self-censorship among activist groups. In all three cases, unjustified spyware use helped governments gain an advantage in preventing future dissent. Victims felt the loss of their ability to express freely, communicate safely, and organize effectively, thereby discouraging them from continuing their advocacy work due to the potential risks involved (Staff 2022).

The existing literature demonstrates how the goal of surveilling these political targets differs around the globe, but an initial pattern shows that **spyware infiltrations are usually part of a comprehensive attack**, which includes arrests or detentions before or after the digital surveillance, smear campaigns, expulsions or isolating the victims (Deibert et al. 2022, Al-Maskati et al. 2022, Rueckert & Schilis-Gallego 2020). As stated by Ahmed Benchemis, communication chief at Human Rights Watch, in an interview with Forbidden Stories: “The point [of surveillance] is presumably to track the private lives of individuals in order to find a hook on which they can hang any big trial” (Rueckert 2021). This was the case for the three case studies, where victims were under surveillance prior to, during, or after prosecution.

The use of spyware as a surveillance method additionally affects both domestic and transnational spaces, as demonstrated by victims’ claims in Spain, Mexico and Western Asia. The individuals targeted suffered a loss of personal autonomy, lived in constant fear of surveillance, and resorted to self-censorship, thereby infringing upon their right to privacy and freedom of expression. Additionally, the consequences of these cases extended beyond national borders. In the Catalonia case, the targeting of European Parliament members raised concerns about democratic values within the European Union. In Western Asia, the spyware attacks targeted civil society members involved in peace mediation, impacting efforts to resolve conflicts. Finally, in Mexico, the spyware affected investigative journalists reporting on organized crime, transcending geographical boundaries. The case studies have demonstrated

how **the use of spyware as a means of surveillance against political dissidents not only violates the human rights of the individuals involved, but also has implications on peacebuilding initiatives, the shrinking civic space, and the suppression of oppositional politics and freedom of expression**.

To sum up, the research project aimed to enrich the existing literature by providing the starting point for a solid and reliable database of victims, clients, tools, and the associated harm, impacts, and human rights violations of spyware attacks. Above all, it represents an avenue for the call to fair justice and accountability for unlawful spyware surveillance. Steven Adair, CEO of the cybersecurity firm Volexity, stated to the Committee to Protect Journalists that "getting a definitive example of spyware that is installed in a phone is 'exceedingly rare'" (Guterl 2022). Moreover, even if the victim is able to prove they have been infected with a specific spyware tool, it is nearly impossible to prove who was responsible for the surveillance (Fakih 2022). This is especially perpetuated by the lack of transparency for intelligence services and states as well as a lack of regulatory frameworks for the spyware market overall. It is thus crucial to contribute to the education of the general public on the dangers of the spyware market through external dissemination.

In this regard, and keeping in mind the limitations in accessing victims' personal information, additional potential target groups that might be relevant to further analyze concern marginalized groups of people, including women and ethnic minorities. Such cases might include the spyware attack in El Salvador targeting 35 journalists and civil society members (Scott-Railton 2022b) or the continuous and transnational spyware attack originating from Rwanda (Scott 2022). Future studies should also examine the definitions and distinctions of spyware purchase and deployment among different governmental regimes, i.e. democratic, authoritarian regimes, etc. Both, the rigorous collection of data and the deeper analysis through case studies help to form a more comprehensive picture on surveillance technology abuse's trends and consequences and on the patterns between victims, customers, and sellers of spyware.

VIII. Bibliography

About Us | Today's latest from Al Jazeera (no date). Available at: https://www.aljazeera.com/about-us.

Abu Sneineh M. (2021). Pegasus: Israel designated Palestinian NGOs "terrorist" to cover hacking tracks, report says. Middle East Eye. http://www.middleeasteye.net/news/pegasus-palestinian-groups-discovered-spyware-hack-and-israel-rushed-outlaw-them.

Access Now (2023) Armenia spyware victims: Pegasus hacking in war. Available at: https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/#case-study.

Access Now. (2020a). "NSO Group WhatsApp hack victims speak out, from India to Rwanda". [online] Available at: https://www.accessnow.org/nso-whatsapp-hacking-victims-stories/.

Access Now. (2020b). "Two years after Khashoggi's slaying, no accountability for spyware firm or Saudi government". [online] Available at: https://www.accessnow.org/khashoggi-two-years-later/.

Access Now. "Human rights leaders at Davos 2022: spyware is a weapon — Press Conference" (no date) Access Now. Available at: https://www.accessnow.org/press-release/spyware-davos-press-conference/.

Agrafiotis, I. et al. (2016). "Cyber Harm: Concepts, Taxonomy and Measurement". Rochester, NY. Available at: https://doi.org/10.2139/ssrn.2828646.

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1).

Al Jazeera Staff. (2021). Palestinian rights activists defiant over Israeli spyware hacks. https://www.aljazeera.com/news/2021/11/14/palestinian-rights-activists-defiant-over-israeli-spyware-hacks.

Al-Maskati, M. et al. (2022) Peace through Pegasus: Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware. Citizen Lab, University of Toronto. Available at: https://citizenlab.ca/2022/04/peace-through-pegasus-jordanian-human-rights-defenders-and-journalists-hacked-with-pegasus-spyware/.

Al-Rawi, A. (2017). Assessing public sentiments and news preferences on Al Jazeera and Al Arabiya. International Communication Gazette, 79(1), pp.26-44.

Al-Rawi, A. (2019). The Gulf Information War | Cyberconflict, Online Political Jamming, and Hacking in the Gulf Cooperation Council. International Journal of Communication, 13, p.22.

Amnesty International (2019a). "Open letter to Novalpina Capital, CC: NSO Group, Francisco Partners". Available at: https://www.amnesty.org/en/latest/research/2019/02/open-letter-to-novalpina-capital-nso-group-and-francisco-partners/.

Amnesty International. (2019b). Morocco: Human Rights Defenders Targeted with NSO Group's Spyware. [online] Available at: https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/.

Associated Press (2019). Report: Slain Mexican journalist's widow targeted by spyware. [online] AP NEWS. Available at: https://apnews.com/article/96ac1993609b4e9d9bbfd3cae60e5153.

Associated Press (2021). Mexico says officials spent $61 million on Pegasus spyware. [online] AP NEWS. Available at: https://apnews.com/article/technology-business-mexico-spyware-8b1784c5ba9dbed2ad39e8746bdf0c81.

Au, Y., (2021). Surveillance as a Service.

BBC (2018). Mexico arrest over murder of reporter Javier Valdez. BBC News. [online] 24 Apr. Available at: https://www.bbc.com/news/world-latin-america-43878097.

BBC (2019). Catalonia's bid for independence from Spain explained. BBC News. https://www.bbc.com/news/world-europe-29478415.

Bellaby, R. (2012). What's the harm? The ethics of intelligence collection. Intelligence and National Security, 27(1), 93-117.

Birks, M., and Mills, J. (2011). Grounded Theory - A Practical Guide. Thousand Oaks: Sage, 1-15.

Campbell, Z., D'Agostino, L. and A.m, 8:00 (2022). Hacked Phones, Undercover Cops, and Conspiracy Theories: Inside Italy's Crackdown on Humanitarian Rescue. [online] The Intercept. Available at: https://theintercept.com/2022/12/21/italy-iuventa-humanitarian-rescue/.

Catalan Gate. (2023). Catalan Gate: Democracy under surveillance. Retrieved from https://catalangate.cat/.

Chan, Anna W (2018). The Need for a Shared Responsibility Regime between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware. Brook. J. Int'l L. 44: 795. Available at: https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1939&context=bjil.

Citizen Lab, Deibert, R., Scott-Railton, J., et al. (2022). CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru. Citizen Lab, University of Toronto. https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/.

Citizen Lab. (2021). Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware. Citizen Lab, University of Toronto. https://citizenlab.ca/2021/11/palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware/

Citizenlab (2020). Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware. The Citizen Lab. Available at: https://citizenlab.ca/2020/08/nothing-sacred-nso-sypware-in-togo/.

Citizenlab (2021). Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware - The Citizen Lab. [online] Available at: https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

Citron, D., & Gray, D. (2012-2013). Addressing the Harm of Total Surveillance: Reply to Professor Neil Richards. Harvard Law Review Forum, 126, 262-274.

Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware, European Parliament, https://www.europarl.europa.eu/committees/en/pega/home/highlights.

Committee to Protect Journalists. (n.d.). Javier Valdez Cárdenas. [online] Available at: https://cpj.org/data/people/javier-valdez-cardenas/.

DeSombre W. et al (2021). Countering cyber proliferation: Zeroing in on Access-as-a-Service. Atlantic Council. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/.

DeSombre, W., et al (2021). A Primer on the Proliferation of Offensive Cyber Capabilities. [online] JSTOR. Available at: https://www.jstor.org/stable/resrep30741.

DeYoung, K. and Nakashima, E. (2017). UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to U.S. intelligence officials, Washington Post, 16 July. Available at: https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html.

Di Salvo, P., (2022). "We Have to Act Like our Devices are Already Infected": Investigative Journalists and Internet Surveillance. Journalism Practice, 16(9), pp.1849-1866.

Earp, M. (2019). CPJ Safety Advisory: Journalist targets of Pegasus spyware. [online] Committee to Protect Journalists. Available at: https://cpj.org/2019/11/cpj-safety-advisory-journalist-targets-of-pegasus/.

Earp, M. (2019b). Indian journalists reported among targets of alleged NSO Group WhatsApp hack. Committee to Protect Journalists, 31 October. Available at: https://cpj.org/2019/10/india-journalists-nso-group-whatsapp-php/ (Accessed: 24 April 2023).

Earp, M. (2021). Pegasus Project revelations show added layer of risk for corruption reporters. [online] Committee to Protect Journalists. Available at: https://cpj.org/2021/07/pegasus-project-risk-corruption-reporters/.Franks, M. (2017). Democratic surveillance. Harvard Journal of Law & Technology (Harvard JOLT), 30(2), 425-490.

Earp, M. (2022). 'The infections were constant:' Julia Gavarrete among dozens of Salvadoran journalists targeted with Pegasus spyware. [online] Committee to Protect Journalists. Available at: https://cpj.org/2022/01/infections-constant-julia-gavarrete-salvadoran-journalists-pegasus-spyware/.

Economist Intelligence Unit. (2022). Democracy Index 2022. [online] Available at: https://www.eiu.com/n/campaigns/democracy-index-2022/.

Editor, C.C. (n.d.). spyware - Glossary | CSRC. [online] csrc.nist.gov. Available at: https://csrc.nist.gov/glossary/term/spyware.

El-Ashy, O., Maroni, I., Mizyed, H., Nammar, R. and Al-Maskati, M. (2019). Big Brother in the Middle-East and North Africa: The expansion of imported surveillance technologies and their supportive legislation.

Esquire (2018). He Dedicated His Career to Exposing the Cartels. Then He Was Gunned Down in the Street. [online] Esquire. Available at: https://www.esquire.com/news-politics/a22996658/javier-valdez-luis-guzman-el-chapo-journalist/.

European Data Protection Supervisor Preliminary Remarks on Modern Spyware (2022), https://edps.europa.eu/data-protection/our-work/publications/papers/edps-preliminary-remarks-modern-spyware_en.

European Parliament (2022). The use of Pegasus and equivalent surveillance spyware - The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware. European Parliament. Available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)740151.

Fakih, L. (2022). I Was Attacked with Pegasus. [online] Human Rights Watch. Available at: https://www.google.com/url?q=https://www.hrw.org/news/2022/01/28/i-was-attacked-pegasus&sa=D&source=docs&ust=1680546948501283&usg=AOvVaw0gvvw8hr_PjtSpVah_3zsd.

Fatafta, M. (2022). Women human rights defenders speak out about Pegasus attacks. [online] Access Now. Available at: https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/.

Feldstein, S. & Kot, B., (2023). Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses. United States of America. Retrieved from https://policycommons.net/artifacts/3524167/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses/4324812/. CID: 20.500.12592/rkqwkm.

Feldstein, Steven; Kot, Brian (2023), Global Inventory of Commercial Spyware & Digital Forensics. Mendeley Data, V10, doi: 10.17632/csvhpkt8tm.10.

Fionnuala Ní Aoláin , Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on- global-regulation-ct-spyware-technology-trade.pdf

Forbiddenstories.org. (n.d.). About The Pegasus Project | Forbidden Stories. [online] Available at: https://forbiddenstories.org/about-the-pegasus-project/.

forbiddenstories.org. (n.d.). Journalists under surveillance. Forbidden Stories. [online] Available at: https://forbiddenstories.org/pegasus-journalists-under-surveillance/.

Forensic Architecture.org. (2020). Forensic Architecture. [online] Available at: https://forensic-architecture.org/investigation/nso-groups-breach-of-private-data-with-fleming-a-covid-19-contact-tracing-software.

Frontline Defenders. (2022). Unsafe Anywhere: Women Human Rights Defenders Speak Out About Pegasus Attacks. Front Line Defenders. https://www.frontlinedefenders.org/en/resource-publication/unsafe-anywhere-women-human-rights-defenders-speak-out-about-pegasus-attacks.

Fuchs, J. (2023). Is the EU protecting people from Pegasus spyware?. Access Now, 17 January. Available at: https://www.accessnow.org/eu-pegasus-spyware/.

Good, Nathaniel, et al. (2005) “Stopping spyware at the gate: a user study of privacy, notice and spyware. Proceedings of the 2005 symposium on Usable privacy and security”. Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=c81f84dc7c9ad16cf68c403ec74a2603b90da9b1.

Guterl, F. (2022). Special report: When spyware turns phones into weapons. [online] Committee to Protect Journalists. Available at: https://cpj.org/reports/2022/10/when-spyware-turns-phones-into-weapons/.

Handler S. (2022) The 5×5—The rise of cyber surveillance and the Access-as-a-Service industry. Atlantic Council, 16 November. Available at: https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-the-rise-of-cyber-surveillance-and-the-access-as-a-service-industry/.

Hedgecoe, G. (2021). Catalan independence talks are back—And the stakes are high for PM Sánchez. Politico EU. https://www.politico.eu/article/catalonia-independence-spain-prime-minister-pedro-sanchez/.

Herrera, Y. M., and Braumoeller, B.F. (2004). Symposium: Discourse and Content Analysis. Qualitative Methods, 2(1): 15-39.

Hoffman, J. (2020). Espionage and repression in the Middle East courtesy of the West. Available at: https://www.opendemocracy.net/en/north-africa-west-asia/espionage-and-repression-middle-east-courtesy-west/.

Hootsen, J.-A. (2022). For Mexican journalists, President López Obrador's pledge to curb spyware rings hollow. [online] Committee to Protect Journalists. Available at: https://cpj.org/2022/10/mexican-journalists-lopez-obradors-pledge-curb-spyware-hollow/.

Human Rights Watch (2021a). "Unchecked Spyware Industry Enables Abuses". [online] Available at: https://www.hrw.org/news/2021/07/30/unchecked-spyware-industry-enables-abuses.

Human Rights Watch. (2021b). The Persecution of Ahmed Mansoor. [online] Available at: https://www.hrw.org/report/2021/01/27/persecution-ahmed-mansoor/how-united-arab-emirates-silenced-its-most-famous-human.

Ignatuschtschenko, E. (2021). Assessing harm from cybercrime. Chapter 8 in Cornish, P. (2021). The Oxford Handbook of Cyber Security. Oxford University Press.

Information for media | Coalition Against Stalkerware (EN). [online] Available at: https://stopstalkerware.org/information-for-media/ [Accessed 3 May 2023].

International Committee of the Red Cross (2022) 'Cyber attack on ICRC: What we know'. Available at: https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know (Accessed: 3 May 2023).

Jili, B. (2022) "Africa: regulate surveillance technologies and personal data", Nature, 607(7919), pp. 445–448. Available at: https://doi.org/10.1038/d41586-022-01949-9.

Jones, M.O. (2023). The New, Unsustainable Order of Arab Digital Autocracy - Disruptions and Dynamism in the Arab World. Carnegie Endowment for International Peace [Preprint]. Available at: https://carnegieendowment.org/2023/05/03/new-unsustainable-order-of-arab-digital-autocracy-pub-89525.

Jones, S. (2017). Catalan ex-president Artur Mas barred from holding public office. The Guardian. https://www.theguardian.com/world/2017/mar/13/catalan-ex-president-artur-mas-barred-from-holding-public-office.

Jones, S. (2022). Catalan president calls for investigation as spyware targets pro-independence leaders. The Guardian. https://www.theguardian.com/world/2022/apr/19/catalan-president-calls-for-investigation-as-spyware-targets-pro-independence-leaders.

Kaspersky (2023) What is zero-click malware, and how do zero-click attacks work? Available at: https://www.kaspersky.com/resource-center/definitions/what-is-zero-click-malware.

Kenyon, M. (2017). Submission to the UN Special Rapporteur on Violence Against Women. Citizen Lab, University of Toronto. Available at: https://citizenlab.ca/2017/11/submission-un-special-rapporteur-violence-women-causes-consequences/.

Khoo, Cynthia, Kate Robertson, and Ronald Deibert. Installing fear: A Canadian legal and policy analysis of using, developing, and selling smartphone spyware and stalkerware applications. (2019). Available at: https://www.citizenlab.ca/docs/stalkerware-legal.pdf

Kirchgaessner, S. and Safi, M. (2020). Dozens of Al Jazeera journalists allegedly hacked using Israeli firm's spyware. The Guardian, 22 December. Available at: https://www.theguardian.com/media/2020/dec/20/citizen-lab-nso-dozens-of-aljazeera-journalists-allegedly-hacked-using-israeli-firm-spyware.

Kirchgaessner, S., & Jones, S. (2020). Phone of top Catalan politician "targeted by government-grade spyware." The Guardian. https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware.

Korff, D. (2016). Harm Caused to Fundamental Rights and Freedoms by State Cybersecurity Interventions. SSRN. http://dx.doi.org/10.2139/ssrn.3709808

Korff, D. (2019). First do no harm: The potential of harm being caused to fundamental rights and freedoms by state cybersecurity interventions. In Research Handbook on Human Rights and Digital Technology (pp. 129-155). Edward Elgar Publishing.

Krapiva N. (2023). Armenia spyware victims: Pegasus hacking in war. Access Now. https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/.

Kumar, Gaurav (2021). An Analysis of the Pegasus Spyware Issue in Light of Surveillance Laws and the Right to Privacy in India. Jus Corpus LJ: 394. Available at: https://heinonline.org/HOL/Page?handle=hein.journals/juscrp2&div=370&g_sent=1&casa_token=gr6tcLfInZsAAAAA:6Sp405SloWJOhv8sCtEbpH0iWvxt4vsdX1fjiiOEaxS0Np6cf18snglO7OtX0Nnamlv62sSzfZc&collection=journals.

Malicious Life. (2019). How is Spyware Legal?. [Cybereason]. Available at: https://open.spotify.com/episode/7arjb9KRbd1ciIOYg06E8c (Accessed: 24 April 2023).

Mansour, Sherif. House Foreign Affairs Committee Tom Lantos Human Rights Commission Briefing on "Human Rights and Freedom of Expression in Morocco." 12 Aug. 2021.

Marczak, B., Abdulemam, A., Scott-Railton, J., Abdul Razzak, B., Anstis, S., Al-Jizawi, N., & Deibert, R. (2022). Pearl 2 Pegasus: Bahraini Activists Hacked with Pegasus Just Days after a Report Confirming Other Victims.

Marczak, B., et al (2018). Hide and Seek Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. [online] Available at: https://nsarchive.gwu.edu/sites/default/files/documents/r95u3s-6c1oa/CitizenLabReport.pdf.

Marczak, B., Scott-Railton, et al (2020). The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit. [online] Available at: https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/#:~:text=The%20personal%20phone%20of%20a.

Moeller, R. (2010). "Spyware. Afterimage: The Journal of Media Arts and Cultural Criticism", 38(1), pp.34–34. doi:https://doi.org/10.1525/aft.2010.38.1.34.

Noguera A.M. (2020). Investigation reveals corruption and illegal interceptions by the Colombian Army. Al Día News. https://aldianews.com/en/politics/policy/corruption-army.

OHCHR (2022). Spyware and surveillance: Threats to privacy and human rights growing, UN report warns. https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report.

OHCHR (2023). Alarming misuse of high-risk technologies in global fight against terrorism says UN expert. Available at: https://www.ohchr.org/en/press-releases/2023/03/alarming-misuse-high-risk-technologies-global-fight-against-terrorism-says.

OHCHR (2023). Spain: UN experts demand investigation into alleged spying programme targeting Catalan leaders. OHCHR. https://www.ohchr.org/en/press-releases/2023/02/spain-un-experts-demand-investigation-alleged-spying-programme-targeting.

OHCHR, What are Human Rights?, United Nations Human Rights Office of the High Commissioner, https://www.ohchr.org/en/what-are-human-rights.

OHCHR. (2019). UAE: UN experts condemn conditions of detention for jailed activist Ahmed Mansoor. [online] Available at: https://www.ohchr.org/en/press-releases/2019/05/uae-un-experts-condemn-conditions-detention-jailed-activist-ahmed-mansoor. .

Olukotun, D. (2017). Spyware in Mexico: an interview with Luis Fernando García of R3D Mexico. [online] Access Now. Available at: https://www.accessnow.org/spyware-mexico-interview-luis-fernando-garcia-r3d-mexico/.

Parsons, C., Molnar, et al. (2017). The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry. [online] Available at: https://citizenlab.ca/docs/stalkerware-holistic.pdf.

Pegg, D. and Cutler, S., (2021). What Is Pegasus and How Does It Hack Phones. The Guardian. Available at: https://www. Theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones.

Phineas Rueckert (2021). Pegasus: The new global weapon for silencing journalists | Forbidden Stories. Available at: https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/.

Phineas Rueckert (2023). When your “friends” spy on you: The firm pitching Orwellian social media surveillance to militaries. Available at: https://forbiddenstories.org/story-killers/osint-s2t-unlocking-cyberspace-journalists-activists/.

Pieper, O. (2021). Pegasus spyware: Mexico one of the biggest targets – DW – 07/22/2021. [online] Deutsche Welle. Available at: https://www.dw.com/en/pegasus-spyware-mexico-one-of-the-biggest-targets/a-58597847.

Platform for the Protection of Journalism and Safety of Journalists, Council of Europe, https://fom.coe.int/en/apropos.

Red en Defensa de los Derechos Digitales (2018). Periodistas de Ríodoce fueron atacados con Pegasus tras el asesinato de Javier Valdez. [online] R3D: Red en Defensa de los Derechos Digitales. Available at: https://r3d.mx/2018/11/27/periodistas-de-riodoce-fueron-atacados-con-pegasus-tras-el-asesinato-de-javier-valdez/.

Reisinger, Payton P. (2022). Through the Spying-Glass: Data Privacy Concerns Regarding Mobile Spyware Apps. Boston College Intellectual Property and Technology Forum. Available at: https://scholar.google.com/scholar_url?url=https://dashboard.lira.bc.edu/downloads/b9d34fdb-775c-4cd3-bdf3-d2d9a118aaa0&hl=de&sa=T&oi=gsb-gga&ct=res&cd=0&d=10356068697146026875&ei=f6gQZJP5IIv2mQHF14nQCg&scisig=AAGBfm29sUiR6Rx_Jzhyr05ZWNEhnbMywQ.

Reporters Without Borders (2022). This is already the deadliest year ever for Mexico’s media | RSF. [online] rsf.org. Available at: https://rsf.org/en/already-deadliest-year-ever-mexico-s-media.

Richards, N. M. (2013). The dangers of surveillance. Harvard Law Review, 126(7), 1934-1965.

Risk Impact: definition, calculation, reduction. (2022). https://www.eclipsesuite.com/risk-severity/.

Roberts, J. and Emma Schroeder (2023). Makings of the Market: Seven perspectives on offensive cyber capability proliferation. Atlantic Council, 1 March. Available at: https://www.atlanticcouncil.org/content-series/tech-at-the-leading-edge/makings-of-the-market-seven-perspectives-on-offensive-cyber-capability-proliferation/.

Rosalili, W. et al. (2021). Non-Criminalization of Cyberstalking and Its Impact on Justice for Victims: Some Evidence from Malaysia. International Journal of Academic Research in Business and Social Sciences. Available at: https://doi.org/10.6007/IJARBSS/v11-i6/10336.

Rozen, J. (2021). ‘There is no private life’: Three Togolese journalists react to being selected for spyware surveillance. Committee to Protect Journalists. https://cpj.org/2021/09/togolese-journalists-spyware-surveillance/.

Sabbagh, D. (2021). Princess Latifa campaigner had ‘phone compromised by Pegasus spyware. The Guardian. https://www.theguardian.com/world/2021/aug/02/princess-latifa-campaigner-david-haigh-phone-compromised-pegasus-spyware.

Schatzberg, E. (2018). Why is there no discipline of technology in the social sciences?. Artefact. Techniques, histoire et sciences humaines, (8), 193-213.Scott, J. (2022) Exonerating Rwanda The Spyware Case of Carine Kanimba. Available at: https://doi.org/10.13140/RG.2.2.18522.41922.

Scott-Railton, J. et al. (2017). Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware. Citizen Lab, University of Toronto. https://citizenlab.ca/2017/07/mexico-disappearances-nso/.

Scott-Railton, J., et al (2020). Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware - The Citizen Lab. [online] citizenlab.ca. Available at: https://citizenlab.ca/2020/08/nothing-sacred-nso-sypware-in-togo/.

Scott-Railton, J., Marczak, B., Anstis, S., Abdul Razzak, B., Crete-Nishihata, M., & Deibert, R. (2019). Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group’s Spyware. Citizen Lab. Available at: https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/.

Scott-Railton, J., Deibert, R., Marczak, B., Poetranto, I., Chanprasert, S. and Abdul Razzak, B. (2022a). GeckoSpy: Pegasus Spyware Used against Thailand’s Pro-Democracy Movement - The Citizen Lab. [online] citizenlab.ca. Available at: https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/.

Scott-Railton, J., Marczak, B., Nigro Herrero, P., Abdul Razzak, B., Al-Jizawi, N., Solimano, S., & Deibert, R. (2022b). Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus

Spyware. The Citizen Lab. [online] citizenlab.ca. Available at: https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/

Shrivastava, Sanskriti, and Muskan Kejriwal (2021). Pegasus Spyware: Evaluating the Need for Surveillance Reform and Introduction of Data Protection Bill. Nirma ULJ 11: 67. https://heinonline.org/HOL/Page?handle=hein.journals/nulj11&div=10&g_sent=1&casa_token=RZtGE8LbYokAAAAA:tNco2e18dvg9VsJi4BqYnC8OQvjK0ns2Y_OFpF6DQEZtia7fXhkTXhzA9_HUbw7CXQ8mJQtVBUA&collection=journals.

Sipior, Janice C., Burke T. Ward, and Georgina R. Roselli (2005). The Ethical and Legal Concerns of Spyware. Information Systems Management: 39-49. Available at: http://130.18.86.27/faculty/warkentin/securitypapers/Merrill/SipiorWardRoselli2005_ISM_Spyware.pdf.

Sosa-Díaz, M.-J., & Valverde-Berrocoso, J. (2022). Grounded Theory as a Research Methodology in Educational Technology. International Journal of Qualitative Methods. https://doi.org/10.1177/16094069221133228.

Southwick, N. and Martínez de la Serna, C. (2022). In 2022, journalist killings continue unabated in Mexico amid a climate of impunity. [online] Committee to Protect Journalists. Available at: https://cpj.org/2022/08/in-2022-journalist-killings-continue-unabated-in-mexico-amid-a-climate-of-impunity/.

Staff, A. (2022). UAE and the impact of spyware on human rights defenders. Americans for Democracy & Human Rights in Bahrain [Preprint]. Available at: https://www.adhrb.org/2022/05/uae-and-the-impact-of-spyware-on-human-rights-defenders/.

Tar, J. (2023). Catalonia bans use of Pegasus spyware. Euractiv. https://www.euractiv.com/section/politics/news/catalonia-bans-use-of-pegasus-spyware/.

Tene, O. (2014). New harm matrix for cybersecurity surveillance. Colorado Technology Law Journal, 12(2), 391-426.

The Wire Staff. (2021). Pegasus: Journalist, Wife Targeted by NSO Spyware, Finds Belgium's Military Intelligence. The Wire. https://thewire.in/tech/pegasus-journalist-wife-targetted-by-nso-spyware-finds-belgiums-military-intelligence.

Tourliere, M. (2021). Gobierno de AMLO pagó 312.8 mdp al empresario que vendió Pegasus a EPN. [online] www.proceso.com.mx. Available at: https://www.proceso.com.mx/nacional/2021/10/28/gobierno-de-amlo-pago-3128-mdp-al-empresario-que-vendio-pegasus-epn-274865.html.

United Nations Economic and Social Commission for Western Asia. (2015). spyware. [online] Available at: https://archive.unescwa.org/spyware.

United Nations Security Management System, Security Policy Manual, 2017, Chapter 4, paragraph 15.

Universal Declaration of Human Rights, https://www.un.org/en/about-us/universal-declaration-of-human-rights.

Unsafe Anywhere: Women Human Rights Defenders Speak Out About Pegasus Attacks (2022). Available at: https://www.frontlinedefenders.org/en/resource-publication/unsafe-anywhere-women-human-rights-defenders-speak-out-about-pegasus-attacks.

Verza, M. (2019). Report: Slain Mexican journalist's widow targeted by spyware. [online] AP NEWS. Available at: https://apnews.com/article/96ac1993609b4e9d9bbfd3cae60e5153.

Warkentin, Merrill, Xin Luo, and Gary F. Templeton (2005). A framework for spyware assessment. Communications of the ACM 48.8: 79-84. Available at: https://www.researchgate.net/publication/220423529_A_framework_for_spyware_assessment

West Asia (no date). Available at: https://asiasociety.org/policy-institute/west-asia.

Wilson, Tamara (2020). Spying on your spouse? The inadequacy of legal protection for intimate partner victims subject to spyware and surveillance technology. Available at: https://ir.wgtn.ac.nz/bitstream/handle/123456789/30465/paper_access.pdf?sequence=1

Wintour, P. (2017). Qatar given 10 days to meet 13 sweeping demands by Saudi Arabia. The Guardian, 27 November. Available at: https://www.theguardian.com/world/2017/jun/23/close-al-jazeera-saudi-arabia-issues-qatar-with-13-demands-to-end-blockade.

Woodhams, S., (2021). Spyware: An unregulated and escalating threat to independent media. Center for International Media Assistance.

Yaakoubi, A.E. (2020). Saudi Arabia takes aim at Muslim Brotherhood before Democrats take over in Washington. Reuters, 18 November. Available at: https://www.reuters.com/article/saudi-security-int-idUSKBN27Y22Y#.

Annex I

An excel sheet of the Event_Target data collection (following pages).

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0001	Spyware incident involving Pegasus being used by Chilean Police Force against journalists.	TAR_0001	Journalist NAME A	Individual	Media	Journalist	Zero-Click exploit	Phone infected for 3 months, exposing senstive information			SOU_0001	EVE_TAR_0001
EVE_0001	Spyware incident involving Pegasus being used by Chilean Police Force against journalists.	TAR_0002	Journalist NAME B	Individual	Media	Journalist	Zero-Click exploit	Phone infected for 3 months, exposing senstive information			SOU_0001	EVE_TAR_0002
EVE_0001	Spyware incident involving Pegasus being used by Chilean Police Force against journalists.	TAR_0003	Unknown_ID_001	Individual	Media	Journalist	Zero-Click exploit	Phone infected for 3 months, exposing senstive information. Target arrested 2 weeks followinig initial infection.			SOU_0001;	EVE_TAR_0003
EVE_0002	Targeted digital attacks against two prominent Moroccan Human Rights Defenders (HRDs) using NSO Group's Pegasus spyware.	TAR_0005	Maati Monjib	Individual	Advocacy	Co-founder	Phishing	Each of the targets were sent spearphishing emails containing malicious links that, if opened, would have installed NetWire, a commercially available spyware.	While between 2017 and 2018 he was targeted through SMS messages carrying malicious links tied to NSO Group, in a report from October 2019 they described how Maati Monjib's phone appeared to have been subjected to malicious redirects while he was navigating the Internet using the Safari browser.		SOU_0002	EVE_TAR_0004
EVE_0002	Targeted digital attacks against two prominent Moroccan Human Rights Defenders (HRDs) using NSO Group's Pegasus spyware.	TAR_0006	Abdessadak El Bouchattaoui	Individual	Legal	Lawyer	Phishing	Each of the targets were sent spearphishing emails containing malicious links that, if opened, would have installed NetWire, a commercially available spyware. They were not successfully infected.			SOU_0002	EVE_TAR_0005
EVE_0003	A coordinated spyware campaign targeting at least nine human rights defenders who been calling for the release of other prominent activists in India	TAR_0007	Nihalsing B Rathod	Individual	Legal	Lawyer	Phishing	Each of the targets were sent spearphishing emails containing malicious links that, if opened, would have installed NetWire, a commercially available spyware. They were not successfully infected.	was targeted multiple times, including with a spyware tools linked to NSO Group		SOU_003	EVE_TAR_0006
EVE_0003	A coordinated spyware campaign targeting at least nine human rights defenders who been calling for the release of other prominent activists in India	TAR_0008	Isha Khandelwal	Individual	Legal	Lawyer	Phishing	Each of the targets were sent spearphishing emails containing malicious links that, if opened, would have installed NetWire, a commercially available spyware. They were not successfully infected.			SOU_003	EVE_TAR_0007
EVE_0003	A coordinated spyware campaign targeting at least nine human rights defenders who been calling for the release of other prominent activists in India	TAR_0009	Degree Prasad Chouhan	Individual	Advocacy	Human Rights Defender	Phishing	Each of the targets were sent spearphishing emails containing malicious links that, if opened, would have installed NetWire, a commercially available spyware. They were not successfully infected.	was targeted multiple times, including with a spyware tools linked to NSO Group		SOU_003	EVE_TAR_0008
EVE_0003	A coordinated spyware campaign targeting at least nine human rights defenders who been calling for the release of other prominent activists in India	TAR_0010	Partho Sarothi Ray	Individual	Educatiion	Associate Professor	Phishing	Each of the targets were sent spearphishing emails containing malicious links that, if opened, would have installed NetWire, a commercially available spyware. They were not successfully infected.			SOU_003	EVE_TAR_0009
EVE_0003	A coordinated spyware campaign targeting at least nine human rights defenders who been calling for the release of other prominent activists in India	TAR_0011	Yug Mohit Chaudhry	Individual	Legal	Criminal Lawyer	Phishing	Each of the targets were sent spearphishing emails containing malicious links that, if opened, would have installed NetWire, a commercially available spyware. They were not successfully infected.			SOU_003	EVE_TAR_0010
EVE_0003	A coordinated spyware campaign targeting at least nine human rights defenders who been calling for the release of other prominent activists in India	TAR_0012	Ragini Ahuja	Individual	Legal	Criminal Lawyer	Phishing	Each of the targets were sent spearphishing emails containing malicious links that, if opened, would have installed NetWire, a commercially available spyware. They were not successfully infected.			SOU_003	EVE_TAR_0011
EVE_0003	A coordinated spyware campaign targeting at least nine human rights defenders who been calling for the release of other prominent activists in India	TAR_0013	PK Vijayan	Individual	Educatiion	Professor	Phishing	Each of the targets were sent spearphishing emails containing malicious links that, if opened, would have installed NetWire, a commercially available spyware. They were not successfully infected.			SOU_003	EVE_TAR_0012
EVE_0003	A coordinated spyware campaign targeting at least nine human rights defenders who been calling for the release of other prominent activists in India	TAR_0014	Jagdalpur Legal Aid Group (JAGLAG)	Non-Governmental Organization (NGO)	Advocacy	Human Rights Collective	Phishing	received malicious e-mails on the group's official ID, which is accessed by all of its members			SOU_003	EVE_TAR_0013
EVE_0003	A coordinated spyware campaign targeting at least nine human rights defenders who been calling for the release of other prominent activists in India	TAR_0015	Journalist	Individual	Media	Journalist	Phishing	Each of the targets were sent spearphishing emails containing malicious links that, if opened, would have installed NetWire, a commercially available spyware. They were not successfully infected.			SOU_003	EVE_TAR_0014
EVE_0004	Following the revelations of the Pegasus Project, Belgium's military intelligence (Service général du renseignement et de la sécurité - SGRS) drew up a list of probable victims, checked their phones and subsequently found signs of an attack using Pegasus spyware on the mobile devices of a Belgian journalist and his wife.	TAR_0016	Peter Verlinden	Individual	Media	Journalist	Unknown	Target states that before the attack they have come under fire from Internet trolls on social media. Quote: "You feel like everyone can watch what you do. It gives a very dirty feeling, a feeling of insecurity. We already tried to live with that, but this is a serious blow on top of it."			SOU_004	EVE_TAR_0015
EVE_0004	Following the revelations of the Pegasus Project, Belgium's military intelligence (Service général du renseignement et de la sécurité - SGRS) drew up a list of probable victims, checked their phones and subsequently found signs of an attack using Pegasus spyware on the mobile devices of a Belgian journalist and his wife.	TAR_0017	Marie Bamutese	Individual	Media	Media practitioner	Unknown	Target states that before the attack they have come under fire from Internet trolls on social media. Investitgation is still	Target 2 might have become victim of smear campaign by Rwandan news outlet.		SOU_004	EVE_TAR_0016

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0005	The target was infected at least 3 times after the publication of a video showing the extrajudicial killing of civilians by the Mexican army in Tamaulipas. The target had spoken to the media about the case.	TAR_0019	Raymundo Ramos Vázquez	Individual	Media	Journalist	Zero-Click exploit	Ramos was infected with Pegasus in August and September 2020. R3D found that the infections occurred after the publication of a video showing the extrajudicial killing of civilians by the Mexican army in Tamaulipas. Ramos had spoken to the media about the case.	During the timeframe of the targeting, Ramos was meeting with representatives of the Office of the United Nations High Commissioner for Human Rights (OHCHR), Mexico's National Human Rights Commission (CNDH), officials from Mexico's Navy and Secretary of Defense, and members of the media.		SOU_007	EVE_TAR_0017
EVE_0006	Target was multiple targeted in 2016, 2017, 2019 and 2020 all in direct relation to covering events about the Mexican government and cartels.	TAR_0018	Ricardo Raphael	Individual	Media	Journalist	Zero-Click exploit	Both Zero-Click (2019-2021) and Phishing (2016-2017) was used. Raphael was first targeted and infected 2016, and again targeted in 2017 during a period of critical reporting on investigations into the Iguala Mass Disappearances (the 43 students disappeared in Ayotzinapa in 2014). In 2019, he was repeatedly infected with Pegasus while on tour for a book that provides a fictionalized account of Los Zetas Cartel and its origins in the Mexican Army. In 2020, he was infected after writing on extrajudicial detentions and official impunity, such as this Washington Post editorial. Not long before he was infected in December 2020, he had accused Mexico's Attorney General of serious misconduct in their investigation of the Iguala Mass Disappearances case. This critique was cited by prominent news outlet Aristegui Noticias the day prior to the hacking.	the 2017 targeting to an operator that we call RECKLESS-1, which also targeted the spouse and colleagues of an assassinated Mexican journalist. Circumstantial evidence connects RECKLESS-1 to the Mexican Government, as the operator was spying exclusively in Mexico.		SOU_007	EVE_TAR_0018
EVE_0007	the device of Mexican opposition lawmaker identified a Pegasus spyware infection, a report by R3D indicates that the infection timeframe coincides with a visit by Colosio Riojas to the Chamber of Deputies (which the target is a member of).	TAR_0020	Agustín Basave Alanís	Individual	Politics	Opposition Lawmaker	Zero-Click exploit	Mexican opposition lawmaker Agustín Basave Alanís identified a Pegasus spyware infection occurring sometime between 2021-09-05 and 2021-09-11. Reporting by Reuters notes that Basave is close to Luis Donaldo Colosio Riojas, who is viewed as a potential presidential candidate for 2024. A report by R3D indicates that the infection timeframe coincides with a visit by Colosio Riojas to the Chamber of Deputies.			SOU_007	EVE_TAR_0019
EVE_0008	Mansoor received SMS text messages on his iPhone promising "new secrets" about detainees tortured in UAE jails if he clicked on an included link. Mansoor asked for help to The Citizen Lab.	TAR_0021	Ahmed Mansoor	Individual	Advocacy	Human rights defender	Phishing	Both phishing and zero-click exploit. On August 10 and 11, 2016, Mansoor received SMS text messages on his iPhone promising "new secrets" about detainees tortured in UAE jails if he clicked on an included link. The links led to a chain of zero-day exploits ("zero-days") that would have remotely jailbroken Mansoor's stock iPhone 6 and installed sophisticated spyware. Once infected, Mansoor's phone would have become a digital spy in his pocket, capable of employing his iPhone's camera and microphone to snoop on activity in the vicinity of the device, recording his WhatsApp and Viber calls, logging messages sent in mobile chat apps, and tracking his movements.	Spyware Infection did not happen as Mansoor noticed and asked Citizen Lab for help.		SOU_008	EVE_TAR_0020
EVE_0009	Phone hacking of 5 Polish individuals involved in politics using Pegasus	TAR_0022	Michal Kolodziejczak	Political Party/Organization	Politics	Farmer and agrarian social movement leader	Zero-Click exploit	Multiple hacks and surveillance			SOU_009	EVE_TAR_0021
EVE_0009	Phone hacking of 5 Polish individuals involved in politics using Pegasus	TAR_0023	Tomasz Szwejgiert	Government Body/Agency/Department	Politics	Collaborated for years with Polish secret services	Zero-Click exploit	Hacked 21 times with Pegasus from late March to June of 2019.			SOU_009	EVE_TAR_0022
EVE_0009	Phone hacking of 5 Polish individuals involved in politics using Pegasus	TAR_0024	Krzysztof Brejza	Political Party/Organization	Politics	Running the opposition's 2019 parliamentary election campaign	Zero-Click exploit	Messages stolen from his phone were doctored and used in a smear campaign against him.			SOU_009	EVE_TAR_0023
EVE_0009	Phone hacking of 5 Polish individuals involved in politics using Pegasus	TAR_0025	Ewa Wrzosek	Individual	Legal	Independent prosecutor	Zero-Click exploit	Multiple hacks and surveillance			SOU_009	EVE_TAR_0024
EVE_0009	Phone hacking of 5 Polish individuals involved in politics using Pegasus	TAR_0026	Roman Giertych	Individual	Legal	Prominent lawyer	Zero-Click exploit	Multiple hacks and surveillance			SOU_009	EVE_TAR_0025
EVE_0010	An International group of experts investigating the 2014 Iguala Mass Disappearance of 43 Mexican students were targeted with Pegasus.	TAR_0027	Interdisciplinary Group of Independent Experts	International Organization	Advocacy		Phishing	In March 2016 a phone belonging to the GIEI group received two messages designed to trick the recipient into clicking. The two messages related to the purported death of a relative. Other attempts followed.		same event as EVE_006, but not the same target	SOU_0010	EVE_TAR_0026
EVE_0011	Journalists based out of Middle East from Al Jazeera and Alaraby TV were targeted by NSO Group's Pegasus. The spying operators mainly- MONARCHY and SNEAKY KESTREL spied on 36 mobile phones. These operatives have been linked with the previous attacks on UAE human rights activist, Ahmed Mansoor.	TAR_0028	Tamer Almisshal	Individual	Media	Journalist	Zero-Click exploit	Multiple kernel panics or phone crashes			SOU_0011	EVE_TAR_0027
EVE_0011	Journalists based out of Middle East from Al Jazeera and Alaraby TV were targeted by NSO Group's Pegasus. The spying operators mainly- MONARCHY and SNEAKY KESTREL spied on 36 mobile phones. These operatives have been linked with the previous attacks on UAE human rights activist, Ahmed Mansoor.	TAR_0029	Rania Dridi	Individual	Media	Journalist	Zero-Click exploit	Multiple hacks and surveillance			SOU_0011	EVE_TAR_0028

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0012	The UAE government used the spyware tool "Karma" with the aid of former US government intelligence operatives to hack the phones of human rights activists, political opponents and foreign leaders.	TAR_0030	Emir Sheikh Tamim bin Hamad al-Thani	Individual	Other	Emir of Qatar	Zero-Click exploit	Device was hacked			SOU_0012	EVE_TAR_0029
EVE_0012	The UAE government used the spyware tool "Karma" with the aid of former US government intelligence operatives to hack the phones of human rights activists, political opponents and foreign leaders.	TAR_0031	Mehmet Şimşek	Individual	Other	Former Deputy Prime Minister of Turkey	Zero-Click exploit	Device was hacked. Found the cyber intrusion "appalling and very disturbing."			SOU_0012	EVE_TAR_0030
EVE_0012	The UAE government used the spyware tool "Karma" with the aid of former US government intelligence operatives to hack the phones of human rights activists, political opponents and foreign leaders.	TAR_0032	Yusuf bin Alawi bin Abdullah	Individual	Other	Former Minister of Foreign Affairs of Oman	Zero-Click exploit	Device was hacked			SOU_0012	EVE_TAR_0031
EVE_0012	The UAE government used the spyware tool "Karma" with the aid of former US government intelligence operatives to hack the phones of human rights activists, political opponents and foreign leaders.	TAR_0033	Tawakkol Karman	Individual	Advocacy	Human Rights Activist; known as "Iron Woman of Yemen"	Zero-Click exploit	Multiple Hacks			SOU_0012	EVE_TAR_0032
EVE_0013	On September to October 2015, Karla Micheel Salas and David Peña are Mexican lawyers and human rights defenders received text messages containing infection attempts with NSO's Pegasus spyware. They were targeted by the government as questions grew about official accounts of the Narvarte killings, and the reported torture, and sexual assault of the victims.	TAR_0034	Karla Micheel Salas	Individual	Legal	Mexican lawyer and human rights defender	Phishing	On October 1, 2015, Salas received a message purporting to inform her of a death and inviting her to a wake. Clicking on the link would have resulted in the infection of her device with NSO's Pegasus exploit infrastructure and spyware.			SOU_0013	EVE_TAR_0033
EVE_0013	On September to October 2015, Karla Micheel Salas and David Peña are Mexican lawyers and human rights defenders received text messages containing infection attempts with NSO's Pegasus spyware. They were targeted by the government as questions grew about official accounts of the Narvarte killings, and the reported torture, and sexual assault of the victims.	TAR_0035	David Peña	Individual	Legal	Mexican lawyer and human rights defender	Phishing	On September 25 and October 15, 2015, Peña received text messages containing infection attempts with NSO's Pegasus spyware. The messages were designed to trick him into clicking on the links. Once clicked, the links would infect Peña's phone. The first message referenced an organization Peña belongs to, the second masqueraded as a "service message". On September 25, 2015, Peña received a "service message" containing a link. Then, on October 15, 2015 he received a message purporting to be a news story revealing audio of a conspiracy to commit extortion by a member of Mexico's Association of Democratic Lawyers (ANAD: Asociación Nacional de Abogados Democráticos, A. C.) and Perla Gomez, the Director of the Human Rights Commission for Mexico City (Comisión de Derechos Humanos del Distrito Federal).			SOU_0013	EVE_TAR_0034
EVE_0014	Three senior Mexican politicians were targeted with infection attempts using Pegasus spyware. All three targets are members of the socially conservative National Action Party (PAN). Between June and July 2016 they were sent text messages containing links to NSO's exploit framework.	TAR_0036	Ricardo Anaya Cortés	Political Party/Organization	Politics	President of Mexico's National Action Party (PAN)	Phishing	Ricardo Anaya Cortés is a lawyer, politician, and current president of PAN. On June 15, 2016 he was sent a text message claiming that he was mentioned in an article in Proceso. Notably, his colleague at PAN, Senator Roberto Gil Zuarth received a nearly identical message on the same day.			SOU_0014	EVE_TAR_0035
EVE_0014	Three senior Mexican politicians were targeted with infection attempts using Pegasus spyware. All three targets are members of the socially conservative National Action Party (PAN). Between June and July 2016 they were sent text messages containing links to NSO's exploit framework.	TAR_0037	Roberto Gil Zuarth	Political Party/Organization	Politics	President of Mexico's Senate (during the targeting)	Phishing	Senator Roberto Gil Zuarth is currently the President of Mexico's Senate and a member of PAN. Between June 15 and 17 2016 he was sent three infection attempts in the form of text messages with links to NSO exploit infrastructure. The messages echoed themes uncovered in prior Citizen Lab reports of targeting in Mexico, such as the death of a father, and a news story in the Mexican news magazine Proceso mentioning the target. A third message suggests that another political party (Party of the Democratic Revolution: PRD) has been critical of him and his colleagues.			SOU_0014	EVE_TAR_0036
EVE_0014	Three senior Mexican politicians were targeted with infection attempts using Pegasus spyware. All three targets are members of the socially conservative National Action Party (PAN). Between June and July 2016 they were sent text messages containing links to NSO's exploit framework.	TAR_0038	Fernando Rodríguez Doval	Political Party/Organization	Politics	Communications Secretary for PAN	Phishing	Fernando Doval is the communications secretary for PAN, having previously served as a legislator representing the Federal District (Mexico City) in the Mexican Congress. On July 14, 2016 he was targeted with an infection attempt via text message.			SOU_0014	EVE_TAR_0037
EVE_0015	The director of a prominent anti-corruption organization Mexicanos Contra la Corrupción y la Impunidad (MCCI) was sent infection attempts with NSO Group's Pegasus spyware. The targeting took place as his organization was working on issues related to offshore holdings and corruption among prominent Mexicans and Mexican government officials.	TAR_0039	Claudio X. González	International Organization	Other	Director of anti-corruption organization	Phishing	On July 27 and August 2 2016, González received text messages as part of a ruse to trick him into clicking on malicious links. If clicked, the messages would have infected his device with NSO Group's Pegasus spyware. The first message, received on July 27th 2016, claimed that he was the subject of negative press coverage by major Mexican newsmagazine, Proceso. The second message, which arrived a few days later on August 2nd, used a similar ruse, but spoke of negative coverage in the newspaper El Universal.			SOU_0015	EVE_TAR_0038

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0016	Wife and colleagues were targeted with NSO Group's Pegasus spyware following the assassination of Javier Valdez, journalist of the newspaper that he founded to investigate cartels and organized crime in Sinaloa, Mexico.	TAR_0040	Griselda Triana	Individual	Media		Phishing	On May 25th and 26th, 2017, eleven days after her husband was slain, Triana received text messages designed to trick her into clicking on malicious links. The messages arrived during a period when she recalls actively cooperating with the authorities investigating his killing, and publicly protesting his death and demanding a serious official investigation. The first infection attempt arrived on May 25th and masqueraded as an update about the killing from Mexican news magazine Proceso. According to the message, the Mexican Office of the Prosecutor (PGR) had announced that his assassination was in fact an attempted carjacking. The idea was farcical and Triana did not click on the link. A day later, Triana received a second infection attempt. The message played on her grief at the loss of her husband and hinted that she might have been attacked in the press. Again, she recalls abstaining from clicking.			SOU_0016	EVE_TAR_0039
EVE_0016	Wife and colleagues were targeted with NSO Group's Pegasus spyware following the assassination of Javier Valdez, journalist of the newspaper that he founded to investigate cartels and organized crime in Sinaloa, Mexico.	TAR_0041	Andrés Villarreal	Individual	Media	Journalist of newspaper founded to investigate cartels and organized crime in Sinaloa, Mexico.	Phishing	Andrés Villarreal received carefully crafted text messages designed to trick them into clicking on exploit links. Clicking on the links would have infected the phone with Pegasus spyware. The first of these messages promised information about the killing of his colleague. The message, disguised as a news alert, stated that the Jalisco New Generation Cartel had been linked to the slaying.			SOU_0016	EVE_TAR_0040
EVE_0016	Wife and colleagues were targeted with NSO Group's Pegasus spyware following the assassination of Javier Valdez, journalist of the newspaper that he founded to investigate cartels and organized crime in Sinaloa, Mexico.	TAR_0042	Ismael Bojórquez	Individual	Media	Journalist of newspaper founded to investigate cartels and organized crime in Sinaloa, Mexico.	Phishing	Ismael Bojórquez received carefully crafted text messages designed to trick them into clicking on exploit links. Clicking on the links would have infected the phone with Pegasus spyware. Same texts as his colleague Villarreal.			SOU_0016	EVE_TAR_0041
EVE_0017	Phones of Palestinian activists working for the human rights NGOs were hacked.	TAR_0043	Ubai al-Aboudi	Individual	Advocacy	Executive Director	Zero-Click exploit	Phone was hacked and monitored.	Aboudi said the violation had affected his daily life because all his contacts were on his phone, as well as his alarm and his diary.	"This is more than just eavesdropping, it's terrifying. The spyware takes complete control over the phone. (...) Whoever is operating the surveillance equipment could phone somebody in the Islamic State and then say I have been dealing with terrorists."	SOU_0017; SOU_0058; SOU_0059; SOU_0060	EVE_TAR_0042
EVE_0017	Phones of Palestinian activists working for the human rights NGOs were hacked.	TAR_0044	Salah Hammouri	Individual	Educatiion	Field researcher	Zero-Click exploit	Phone was hacked and monitored.	He is facing deportation after the Israeli Interior Ministry announced the revocation of his Jerusalem residency permit on the grounds of "breach of allegiance to the State of Israel". Afraid of being arrested and/or deported, he has been forced to relocate to Ramallah.		SOU_0017; SOU_0058; SOU_0059; SOU_0060	EVE_TAR_0043
EVE_0018	Amnesty International reports that one of their researchers, as well as a Saudi activist based abroad, received suspicious SMS and WhatsApp messages in June 2018.	TAR_0045	Amnesty International researcher	Non-Governmental Organization (NGO)	Advocacy		Phishing	Text messages carried links to domains already identified as part of that same network infrastructure used by NSO Group or its customers to deliver exploits and malware designed to silently harvest data from the victims' phones. This malware would allow an attacker complete access to the target's phone or computer, essentially turning the device into a sophisticated eavesdropping and tracking tool to be used against them.			SOU_0018	EVE_TAR_0044
EVE_0018	Amnesty International reports that one of their researchers, as well as a Saudi activist based abroad, received suspicious SMS and WhatsApp messages in June 2018.	TAR_0046	Amnesty International Saudi activist based abroad	Non-Governmental Organization (NGO)	Advocacy		Zero-Click exploit				SOU_0018	EVE_TAR_0045
EVE_0019	In 2016-17 two prominent Mexican journalists were targeted by NSO Group's Pegasus spyware. The attack was suspected to be an act of "political spying" committed by public officials of the Mexican Govt.	TAR_0047	Jorge Carrasco	Individual	Media	Editor-in-chief	Phishing	The same phone number was used to send multiple text messages contaning malicious links to both the journalists in an act to intimidate them.			SOU_0019	EVE_TAR_0046
EVE_0019	In 2016-17 two prominent Mexican journalists were targeted by NSO Group's Pegasus spyware. The attack was suspected to be an act of "political spying" committed by public officials of the Mexican Govt.	TAR_0048	Carmen Aristegui	Individual	Media	Investigative journalist	Phishing	The same phone number was used to send multiple text messages contaning malicious links to both the journalists in an act to intimidate them.			SOU_0019	EVE_TAR_0047
EVE_0020	the target was summoned by the Moroccan police on June 25th, for a tweet that ciritized the judicial system in a case against protestors from Hirak el-Rif. Amnesty later found proof that the target was surveillance during the same period he was prosecuted.	TAR_0049	Omar Radi	Individual	Media	Head of Investigations	Phishing	used the same network injection attacks that were first observed against Maati Monjib. the phone was targeted and put under surveillance during the same period as he was prosecuted. All injections happened while using the LTE/4G mobile connection. network injection attacks which manipulated unencrypted web traffic in order to force Maati Monjib's browser to visit an exploitation site, located at the domain free247downloads[.]com. injection attacks occurred on 27th January, 11th February, and 13th of September 2019.	Amnesty's analysis of Omar's phone revealed traces of similar network injections as recently as 29th January 2020. These most recent attempts involved the new, previously undisclosed, domain name urlpush[.] net.	Additionally to the digital surveillance, Radi was summoned by the police seven times. The multiple summonses, each resulting in 6 to 9 hours-long interrogation sessions, appear to be aimed at exerting psychological pressure on Radi, possibly in retaliation for his journalistic work.	SOU_0020; SOU_0021	EVE_TAR_0048

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0022	The telephone number of an intelligence officer at the Special Service for National Security (SSNS) of Hungary, which conducts secret surveillance and interceptions, appears in the list of Pegasus spyware targets in Hungary.	TAR_0080	Intelligent officer	Government Body/Agency/Department	Other	Intelligence officer at the Special Service for National Security (SSNS) of Hungary	Zero-Click exploit	It is unclear why this SSNS telephone number was selected for targeting. There are two plausible explanations. One is that the intelligence officer himself became a target for some reason. The other is that Pegasus is operated by SSNS and it was only installed on the employee's phone for testing purposes. Both explanations further reinforce previous information that Pegasus is used against Hungarian targets by Hungary's government agencies.			SOU_0028	EVE_TAR_0049
EVE_0023	A Vietnamese hacking group known as OceanLotus or APT32 has been targeting human rights groups and activists in the country through surveillance. It has been alleged that the group is leaking private information of activists, NGOs, etc to the Government.	TAR_0081	Bui Thanh Hieu	Individual	Advocacy	Pro-Democracy Human Rights Activist and Blogger	Phishing	Bui Thanh Hieu writes on human rights and economic justice in Vietnam and was targeted four times between February 2018 and December 2019			SOU_0029	EVE_TAR_0050
EVE_0023	A Vietnamese hacking group known as OceanLotus or APT32 has been targeting human rights groups and activists in the country through surveillance. It has been alleged that the group is leaking private information of activists, NGOs, etc to the Government.	TAR_0082	Vietnamese Overseas Initiative for Conscience Empowerment (VOICE)	Non-Governmental Organization (NGO)	Advocacy	Non-profit organisation registered in the US that works to promote civil society, support refugee settlement and advocacy in Southeast Asia with a special focus on Vietnam.	Phishing	The suspected reason behind the attack could be attributed to the VOICE's work in Vietnamese refugees resettling.			SOU_0029	EVE_TAR_0051
EVE_0023	A Vietnamese hacking group known as OceanLotus or APT32 has been targeting human rights groups and activists in the country through surveillance. It has been alleged that the group is leaking private information of activists, NGOs, etc to the Government.	TAR_0083	Anonymous Blogger	Individual	Media	Blogger	Phishing	The victim's identity was hidden by Amnesty for safety purposes. There is no information as to how the victim was targeted but one of the reasons that could be attributed to the attack is that, the victim wrote about a violent police clash that happened in Vietnam in 2009. Since this is an act of dissent hence, they would have been targeted for the same.			SOU_0029	EVE_TAR_0052
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0050	Jutatip Sirikhan	Individual	Advocacy	Key Member and President	Zero-Click exploit	The Citizen Lab observed evidence of an infection of her phone on or around October 21, 2020, one of the first infection dates found in this investigation. She was again hacked on March 18, 2021, just two days before a planned protest calling for reforms to the monarchy was scheduled on March 20, 2021 in Bangkok. They determined her device was infected a total of six times.	On November 23, 2021, Apple began sending notifications to iPhone users targeted by state-backed attacks with mercenary spyware. The recipients included individuals that Apple believes were targeted with NSO Group's FORCEDENTRY exploit.	this an all following cases from the same event: Forensic evidence from the examined devices indicates that two zero-click exploits were used against the phones we examined: the KISMET and FORCEDENTRY exploits. We saw no evidence of one-click exploits used.	SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0030	EVE_TAR_0053
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0051	Poramin Rassameesawas	Individual	Advocacy	Member	Zero-Click exploit	Other FreeYOUTH members and close affiliates who were also infected with Pegasus			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0031	EVE_TAR_0054
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0052	Katekanok Wongsapakdee	Individual	Advocacy	Member	Zero-Click exploit	Infected once on or around 2021-09-05			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0032	EVE_TAR_0055
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0053	Pansiree Jirathakoone	Individual	Advocacy	Member	Zero-Click exploit	Infected once on or around 2021-08-17			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0033	EVE_TAR_0056
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0054	Chatrapee Artsomboon	Individual	Advocacy	Member	Zero-Click exploit	Infected twice on or around 2021-08-30 and 2021-09-09			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0034	EVE_TAR_0057
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0055	Piyarat Chongthep	Individual	Advocacy	Member	Zero-Click exploit	was infected with Pegasus, according to forensic indicators present on the device, although the exact date of the infection could not be determined at the time of analysis.			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0035	EVE_TAR_0058
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0056	Rattapoom Lertpaijit	Individual	Advocacy	Member	Zero-Click exploit	multiple members of the Members of We Volunteer (WEVO) were infected with Pegasus. The group is often referred to as "Guard WEVO," as they provide support to other protest groups. This target was infected between August and September 2021.	According to the group's official Facebook page, at the time of infection, at least 66 WEVO members were charged with multiple offenses, including violations of the Emergency Decree, and illegal association. Piyarat was also charged for committing a lèse-majesté offense.		SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0036	EVE_TAR_0059
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0057	Wichapat Srigasipun	Individual	Advocacy	Member	Zero-Click exploit	were infected between August and September 2021.			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0037	EVE_TAR_0060

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0058	Panusaya "Rung" Sithijirawattanakul	Individual	Advocacy	Member	Zero-Click exploit	At least four members of the United Front of Thammasat and Demonstration (UFTD), a prominent youth movement from Thammasat University in Bangkok, were infected with Pegasus. Citizen Lab analysis revealed that Panusaya was repeatedly hacked with Pegasus throughout June (15, 20, and 23), and again on or around September 24, 2021.	The hacking coincided with renewed pro-democracy protests in Thailand.		SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0038	EVE_TAR_0061
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0059	Niraphorn Onnkhaow	Individual	Advocacy	Member	Zero-Click exploit	Niraphorn, meanwhile, was infected with Pegasus at least 12 times between February and June 2021. Some of the infections took place shortly before protests, such as an infection on March 19, 2021, just days before a Bangkok protest that demanded political reforms and the release of protest leaders.	This hacking is especially interesting given that she played a support role in protest organizing, rather than serving as a protest leader. For example, Niraphorn is known as a co-registrant of the UFTD's bank account that is used to accept donations.	highest amount of infections for this event	SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0039	EVE_TAR_0062
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0060	Nutchanon Pairoj	Individual	Advocacy	Member	Zero-Click exploit	During the periods when Panusaya was jailed, Nutchanon and Benja assisted in the UFTD's leadership. In November 2021, Nutchanon and Benja were sentenced to contempt of court. Both were infected with Pegasus in November 2021. Nutchanon's phone, meanwhile, was infected on November 18, 2021.			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0040	EVE_TAR_0063
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0061	Chonlatit Chottsawas	Individual	Advocacy	Member	Zero-Click exploit	Inected once on or around 2021-09-23			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0041	EVE_TAR_0064
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0062	Benja Apan	Individual	Advocacy	Former Member and Leader	Zero-Click exploit	During the periods when Panusaya was jailed, Nutchanon and Benja assisted in the UFTD's leadership. In November 2021, Nutchanon and Benja were sentenced to contempt of court. Both were infected with Pegasus in November 2021. Benja's phone was infected on November 17, 2021. Benja's device was infected with Pegasus while she was in detention after being arrested on October 7, 2021.	She spent 99 days in prison after being repeatedly denied bail for lèse-majesté and other offenses. The phone was not in her custody during this period.		SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0042	EVE_TAR_0065
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0063	Jatupat Boonpattararaksa	Individual	Advocacy	Activist	Zero-Click exploit	Jatupat was repeatedly infected with Pegasus in 2021, in June and July (on or around June 23, 28, and July 9, 2021), a period during which pro-democracy protests had resumed. Jatupat had also organized a pro-democracy protest in Khon Kaen on July 1, 2021.	Jatupat led the "Thalufah" ("Through the Sky") pro-democracy group		SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0043	EVE_TAR_0066
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0064	Arnon Nampa	Individual	Legal	Lawyer and Activist	Zero-Click exploit	Arnon was infected with Pegasus multiple times throughout 2020 and 2021. The first detected infection occurred on or around December 3, 2020, just days after he was charged alongside other activists with insulting the monarchy. A second infection took place less than two weeks later on December 15, 2020. He was subsequently arrested. He spent 113 days in jail. Arnon was again infected with Pegasus on or around July 14, 2021, shortly before a large-scale protest, and on the same day that he was quoted in a Bloomberg article. While he was in custody, his phone, which he did not have in his possession at time of his arrest, but remained active, was hacked with Pegasus on or around August 31, 2021.	Arnon Nampa is a leading human rights lawyer and protest leader. His work has included defending activists accused of lèse-majesté, and publicly calling for the repeal of the law. He was charged with at least 14 lèse-majesté charges and was detained for a total of 339 days between 2020-2022.		SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0044	EVE_TAR_0067
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0065	Inthira Charoenpura	Individual	Other	Actor	Zero-Click exploit	Inthira Charoenpura, who spoke out publicly in support of protests and donated water and other supplies, was repeatedly infected with Pegasus throughout April and June 2021 (April 9 and 26; June 4, 2021). Inthira has reportedly faced charges of lèse-majesté and sedition.	Speculatively, her role as a fundraiser for anti-government protests may have triggered the targeting, as she used her social media account to call for public donations and used a bank account under her own name.		SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0045	EVE_TAR_0068
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0066	Individual #3	Other	Advocacy	Protestor	Zero-Click exploit	Three members from an anonymous group of individuals that contributed funds to help support the protests, which we refer to as "the Mad Hatter" as a pseudonym in this report, were also infected with Pegasus. These individuals stated that they have often joined the protests as participants, but have never served as organizers or speakers.			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0046	EVE_TAR_0069
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0067	Dechathorn Bamrungmuang	Individual	Other	Rapper, Founder	Zero-Click exploit	Dechathorn Bamrungmuang, a popular rapper known by the stage name "Hockhacker," was arrested and charged with sedition and other offenses after performing at a pro-democracy protest. Dechatorn's device was hacked with Pegasus on or around August 18, 2021, almost one year after his 2020 arrest.	As a founder of the "Rap Against Dictatorship" (RAD) group, Dechathorn writes lyrics that are critical of the government and detail political problems in the country.		SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0047	EVE_TAR_0070
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0068	Elia Fofi	Individual	Advocacy	Activist	Zero-Click exploit	Infected once on or around 2021-08-17			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0048	EVE_TAR_0071

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0069	Nuttaa Mahattana	Individual	Advocacy	Activist	Zero-Click exploit	Infected once on or around 2021-09-23			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0049	EVE_TAR_0072
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0070	Yingcheep Atchanont	Individual	Advocacy	Lawyer	Zero-Click exploit	Infected ten times on or around 2020-11-28 2020-12-01 2020-12-08 2021-02-10 2021-02-16 2021-03-04 2021-03-16 2021-04-23 2021-06-20 2021-11-12			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0050	EVE_TAR_0073
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0071	Individual #4	Individual	Advocacy	Protestor	Zero-Click exploit	Three members from an anonymous group of individuals that contributed funds to help support the protests, which we refer to as "the Mad Hatter" as a pseudonym in this report, were also infected with Pegasus. These individuals stated that they have often joined the protests as participants, but have never served as organizers or speakers.			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0051	EVE_TAR_0074
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0072	Individual #5	Individual	Advocacy	Protestor	Zero-Click exploit	Three members from an anonymous group of individuals that contributed funds to help support the protests, which we refer to as "the Mad Hatter" as a pseudonym in this report, were also infected with Pegasus. These individuals stated that they have often joined the protests as participants, but have never served as organizers or speakers.			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0052	EVE_TAR_0075
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0073	Bussarin Paenaeh	Individual	Advocacy	Lawyer	Zero-Click exploit	Infected once on or around 2021-02-17			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0053	EVE_TAR_0076
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0074	Pornpen Khongkachonkiet	Individual	Advocacy	HRD	Zero-Click exploit	Infected once on or around 2021-11-16			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0054	EVE_TAR_0077
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0075	Puangthong Pawakapan	Individual	Advocacy	Academic	Zero-Click exploit	Infected five times on or around: 2021-05-31, 2021-06-10, 2021-06-25, 2021-06-30, 2021-07-02			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0055	EVE_TAR_0078
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0076	Prajak Kongkirati	Individual	Advocacy	Academic	Zero-Click exploit	Infected twice or or around 2021-06-14 and 2021-07-02			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0056	EVE_TAR_0079
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0077	Sarinee Achavanuntakul	Individual	Advocacy	Academic	Zero-Click exploit	Infected on or around 2021-09-15			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0057	EVE_TAR_0080
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0078	Individual #2	Individual	Advocacy	Activist	Zero-Click exploit	were infected once between August and September 2021 (on or around 2021-08-18)			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0058	EVE_TAR_0081
EVE_0021	Extensive espionage campaign targeting Thai pro-democracy protesters, and activists calling for reforms to the monarchy. at least 30 individuals were infected with NSO Group's Pegasus spyware.	TAR_0079	Individual #1	Individual	Advocacy	Activist	Zero-Click exploit	Infected once on 2021-11-17			SOU_0022; SOU_0023; SOU_0024; SOU_0025; SOU_0026; SOU_0027; SOU_0030	EVE_TAR_0082
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0084	Noah Bullock	Individual	Advocacy		Zero-Click exploit	Infected thrice on or around 2021-09-04 2021-09-28 2021-11-12	CL assesses that at least two zero-click exploits were deployed against the journalists in El Salvador: KISMET and FORCEDENTRY. Thirteen of the phones contained the KISMET FACTOR, which we believe is an artifact left behind by the execution of NSO Group's zero-click KISMET exploit. Additionally, In the case of a single target at El Faro, CL saw one-click SMS messages sent to the target containing links matching our Pegasus fingerprint.		SOU_0031; SOU_0032	EVE_TAR_0083
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0085	Ricardo Avelar	Individual	Media	Journalist	Zero-Click exploit	Infected ten times on or around 2020-08-31 2020-09-22 2021-02-21 2021-03-16 2021-03-26 2021-04-27 2021-06-15 2021-07-14 2021-09-04 2021-09-12			SOU_0031; SOU_0032	EVE_TAR_0084

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0086	Ana Beatriz Lazo	Individual	Media	Journalist	Zero-Click exploit	Infected once on or around 2021-10-04			SOU_0031; SOU_0032	EVE_TAR_0085
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0087	Carlos Dada	Individual	Media	Journalist	Zero-Click exploit	Infected twelve times: sometime between 2020-07-08 - 2021-06-09			SOU_0031; SOU_0032	EVE_TAR_0086
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0088	Carlos Ernesto Martínez D' aubuisson	Individual	Media	Journalist	Zero-Click exploit	was targeted by TOROGOZ in an unsuccessful attempt with the FORCEDENTRY exploit. The exploit was fired at a non-vulnerable version of iOS. Was targeted 28 times sometime between 2020-06-29 and 2021-10-21			SOU_0031; SOU_0032	EVE_TAR_0087
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0089	Daniel Lizárraga	Individual	Media	Journalist	Zero-Click exploit	Was infected 8 times, between 2021-04-12 and 2021-07-08			SOU_0031; SOU_0032	EVE_TAR_0088
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0090	Daniel Reyes	Individual	Media	Journalist	Zero-Click exploit	was infected twice between 2020-10-01 and 2021-11-04			SOU_0031; SOU_0032	EVE_TAR_0089
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0091	Efren Lemus	Individual	Media	Journalist	Zero-Click exploit	was infected ten times between 2021-04-23 and 2021-09-25			SOU_0031; SOU_0032	EVE_TAR_0090
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0092	Gabriel Labrador	Individual	Media	Journalist	Zero-Click exploit	was infected 20 times between 2020-08-06 and 2021-11-11			SOU_0031; SOU_0032	EVE_TAR_0091
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0093	Gabriela Cáceres	Individual	Media	Journalist	Zero-Click exploit	was infected 13 times between 2021-04-17 and 2021-09-24			SOU_0031; SOU_0032	EVE_TAR_0092
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0094	José Luis Sanz	Individual	Media	Journalist	Zero-Click exploit	was infected 13 times between 2020-07-04 and 2020-12-19			SOU_0031; SOU_0032	EVE_TAR_0093
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0095	Julia Gavarrete	Individual	Media	Journalist	Zero-Click exploit	was infected 18 times between 2021-02-23 and 2021-09-09 on two different phones. Quote from Julia: "Anything sensitive that they want to say to me, they can only say in person. This is one of the most significant pressures that I have had to deal with. I was cautious before, but [now] I am even more extreme to avoid putting sources in danger. But it wears you out day-to-day, and you have to make an even greater effort to be able to produce journalism."			SOU_0031; SOU_0032; SOU_0037	EVE_TAR_0094
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0096	María Luz Nóchez	Individual	Media	Journalist	Zero-Click exploit	was infected 3 times between 2021-02-17 and 2021-06-09			SOU_0031; SOU_0032	EVE_TAR_0095
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0097	Mauricio Ernesto Sandoval Soriano	Individual	Media	Journalist	Zero-Click exploit	was infected 4 times between 2020-08-19 and 2021-10-01			SOU_0031; SOU_0032	EVE_TAR_0096

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0098	Nelson Rauda	Individual	Media	Journalist	Zero-Click exploit	was infected 6 times between 2021-04-30 and 2021-09-10			SOU_0031; SOU_0032	EVE_TAR_0097
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0099	Óscar Martínez	Individual	Media	Journalist	Zero-Click exploit	was infected 42 times between 2020-07-15 and 2021-10-30		42 times!	SOU_0031; SOU_0032	EVE_TAR_0098
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0100	Rebeca Monge	Individual	Media	Journalist	Zero-Click exploit	was infected once on or around 2021-10-07			SOU_0031; SOU_0032	EVE_TAR_0099
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0101	Roman Gressier	Individual	Media	Journalist	Zero-Click exploit	was infected 4 times between 2021-05-17 and 2021-06-23			SOU_0031; SOU_0032	EVE_TAR_0100
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0102	Roxana Lazo	Individual	Media	Journalist	Zero-Click exploit	was infected 12 times between 2021-04-19 and 2021-11-02			SOU_0031; SOU_0032	EVE_TAR_0101
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0103	Sergio Arauz	Individual	Media	Journalist	Zero-Click exploit	was infected 14 times between 2020-08-12 and 2021-10-21			SOU_0031; SOU_0032	EVE_TAR_0102
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0104	Valeria Guzmán	Individual	Media	Journalist	Zero-Click exploit	was infected 8 times between 2020-07-04 and 2021-11-19			SOU_0031; SOU_0032	EVE_TAR_0103
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0105	Víctor Peña	Individual	Media	Journalist	Zero-Click exploit	was infected once sometime between 2021-11-22 and 2021-11-23			SOU_0031; SOU_0032	EVE_TAR_0104
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0106	Jose Marinero	Individual	Advocacy		Zero-Click exploit	was infected 2 times between 2021-04-08 and 2021-09-12			SOU_0031; SOU_0032	EVE_TAR_0105
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0107	Xenia Hernandez	Individual	Advocacy		Zero-Click exploit	was infected 17 times between 2021-02-23 and 2021-11-16			SOU_0031; SOU_0032	EVE_TAR_0106
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0108	Beatriz Benitez	Individual	Media	Journalist	Zero-Click exploit	was infected once on or around 2021-07-01			SOU_0031; SOU_0032	EVE_TAR_0107
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0109	Ezequiel Barrera	Individual	Media	Journalist	Zero-Click exploit	was infected 9 times between 2020-09-10 and 2021-09-19			SOU_0031; SOU_0032	EVE_TAR_0108

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0110	Xenia Oliva	Individual	Media	Journalist	Zero-Click exploit	was infected 7 times between 2020-11-12 and 2021-11-04			SOU_0031; SOU_0032	EVE_TAR_0109
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0111	Oscar Luna	Individual	Media	Journalist	Zero-Click exploit	was infected twice between 2021-04-18 and 2021-09-29			SOU_0031; SOU_0032	EVE_TAR_0110
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0112	Mariana Belloso	Individual	Media	Journalist	Zero-Click exploit	was infected twice between 2021-09-29 and 2021-10-09			SOU_0031; SOU_0032	EVE_TAR_0111
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0113	Carmen Tatiana Marroquín	Individual	Media	Journalist	Zero-Click exploit	was infected once on or around 2021-09-05			SOU_0031; SOU_0032	EVE_TAR_0112
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0114	Individual #1	Individual	Media	Journalist	Zero-Click exploit	was infected twice between 2021-06-03 and 2021-06-30			SOU_0031; SOU_0032	EVE_TAR_0113
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0115	Individual #2	Individual	Media	Journalist	Zero-Click exploit	was infected 3 times between 2020-09-09 and 2020-11-26			SOU_0031; SOU_0032	EVE_TAR_0114
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0116	Individual #3	Individual	Media	Journalist	Zero-Click exploit	was infected 3 times between 2020-09-07 and 2021-05-21			SOU_0031; SOU_0032	EVE_TAR_0115
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0117	Individual #4	Individual	Media	Journalist	Zero-Click exploit	was infected once on or around 2021-09-27			SOU_0031; SOU_0032	EVE_TAR_0116
EVE_0024	Confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. The targes were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang	TAR_0118	Individual #5	Individual	Advocacy	Unknown	Zero-Click exploit	was infected once on or around 2021-05-21			SOU_0031; SOU_0032	EVE_TAR_0117
EVE_0025	Saudi activists based in London and that were in frequent contact with the journalist Khashoggi, who was infamously killed at the Saudi Arabian embassy in Istanbul in October 2018, were targeted with Pegasus.	TAR_0119	Ghanem Almasarir	Individual	Media	YouTube comic and satirist	Phishing	The evidence Almasarir phone was a target came in the form of a June 23 message that appeared to have been sent by DHL. It looked like the kind of delivery message people across the world receive every day, telling him he had a package arriving on the 28th. It also contained a shortened link where he could manage his delivery. But clicking on that link would've led to the installation of the Pegasus tool, capable of hoovering up data within.			SOU_0033	EVE_TAR_0118
EVE_0025	Saudi activists based in London and that were in frequent contact with the journalist Khashoggi, who was infamously killed at the Saudi Arabian embassy in Istanbul in October 2018, were targeted with Pegasus.	TAR_0120	Omar Abdulaziz	Individual	Advocacy	Human rights activist	Phishing	Almasarir's phone was targeted with text messages warning of a package delivery. Almasarir is wary of such messages and says he never clicks on links from unknown senders. The initial panic subsides, as he talks about how he deals with an constant assault on his online life. He claims his YouTube account has repeatedly been the subject of removal requests; his Instagram hacked and deleted; alerts on his phone often warn him that someone, somewhere, is trying to access his Google and Twitter accounts.			SOU_0033	EVE_TAR_0119

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0025	Saudi activists based in London and that were in frequent contact with the journalist Khashoggi, who was infamously killed at the Saudi Arabian embassy in Istanbul in October 2018, were targeted with Pegasus.	TAR_0121	Yahya Assiri	Non-Governmental Organization (NGO)	Advocacy	Founder of Saudi Arabian human rights organization ALQST	Phishing	In May 2018, a strange message from a German number told Assiri he was due to appear in court due to "participation in suspicious meetings seeking to undermine the Kingdom" (Back in December 2017, Assiri organized ALQST's first conference in London). Fearing the link within was malicious, he opened it on an Apple Mac that he didn't mind being infected. It led to what appeared to be the official website of the Saudi Arabian Minister for Justice, leading Assiri to believe it legitimate. He later opened the link on his iPhone. Shortly after, strange things began happening to his Apple devices. First, his iPhone started heating up as it burned through the battery. When he tried to restart the phone, it wouldn't come back on. Later, he attempted to retrieve a backup from his Mac, but the computer simply froze after that request.			SOU_0033	EVE_TAR_0120
EVE_0026	Colombian army illegal intercepted communications from senior judges, politicians and journalists through a technological platform called Invisible Man bought from the Spanish company Mollitiam Industries, dedicated to cyber-intelligence.	TAR_0122	Camilo Romero	Government Body/Agency/Department	Politics	Former Nariño Governor	Zero-Click exploit	Communications intercepted through Invisible Man platform. The system, "allows you to do everything: enter any computer, access calls and conversations from WhatsApp and Telegram Web, download archived or deleted chat conversations, photos, and in general whatever is stored in the memory of the infected machine." Journalists who worked on this investigation were heavily and extensively followed and threatened.			SOU_0034	EVE_TAR_0121
EVE_0026	Colombian army illegal intercepted communications from senior judges, politicians and journalists through a technological platform called Invisible Man bought from the Spanish company Mollitiam Industries, dedicated to cyber-intelligence.	TAR_0123	Roy Barreras	Government Body/Agency/Department	Politics	Senator	Zero-Click exploit	Communications intercepted through Invisible Man platform. The system, "allows you to do everything: enter any computer, access calls and conversations from WhatsApp and Telegram Web, download archived or deleted chat conversations, photos, and in general whatever is stored in the memory of the infected machine." Journalists who worked on this investigation were heavily and extensively followed and threatened.			SOU_0034	EVE_TAR_0122
EVE_0026	Colombian army illegal intercepted communications from senior judges, politicians and journalists through a technological platform called Invisible Man bought from the Spanish company Mollitiam Industries, dedicated to cyber-intelligence.	TAR_0124	César Reyes	Government Body/Agency/Department	Legal	Magistrate of the Colombian Supreme Court	Zero-Click exploit	Communications intercepted through Invisible Man platform. The system, "allows you to do everything: enter any computer, access calls and conversations from WhatsApp and Telegram Web, download archived or deleted chat conversations, photos, and in general whatever is stored in the memory of the infected machine." Journalists who worked on this investigation were heavily and extensively followed and threatened.			SOU_0034	EVE_TAR_0123
EVE_0026	Colombian army illegal intercepted communications from senior judges, politicians and journalists through a technological platform called Invisible Man bought from the Spanish company Mollitiam Industries, dedicated to cyber-intelligence.	TAR_0125	Cristina Lombana	Government Body/Agency/Department	Legal	Magistrate of the Colombian Supreme Court	Zero-Click exploit	Communications intercepted through Invisible Man platform. The system, "allows you to do everything: enter any computer, access calls and conversations from WhatsApp and Telegram Web, download archived or deleted chat conversations, photos, and in general whatever is stored in the memory of the infected machine." Journalists who worked on this investigation were heavily and extensively followed and threatened.			SOU_0034	EVE_TAR_0124
EVE_0027	Two kinds of commercial spyware on the phone of a leading exiled Egyptian dissident were found. One piece of malware recently found on an iPhone belonging to Ayman Nour, a dissident and 2005 Egyptian presidential candidate who subsequently spent three years in jail, originated with Pegasus. TThe other was from from a company called Cytrox, which also has Israeli ties. This was the first documentation of a hack by Cytrox, a little-known NSO Group rival.	TAR_0126	Ayman Nour	Individual	Politics	Exiled dissident and 2005 Egyptian presidential candidate	Zero-Click exploit	Both instances of malware were simultaneously active on the phone. They proceeded to turning the smartphone into an eavesdropping device and siphoning out its vital data. One captured module records all sides of a live conversation.			SOU_0035	EVE_TAR_0125
EVE_0028	Turkish officials had used the program "Finspy" by Finfisher to spy on members of the opposition party CHP. The software was primarily used during a three-week protest against Turkish President Recep Erdogan organized by CHP leader Kemal Kilicdaroglu in July 2017.	TAR_0127	Members of the Turkish opposition party Republican People's Party (CHP) (Unknown_ID_011)	Political Party/Organization	Politics	Turkish opposition party Republican People's Party (CHP)	Zero-Click exploit	The software was primarily used during a three-week protest against Turkish President Recep Erdogan organized by CHP leader Kemal Kilicdaroglu in July 2017. Fake Twitter accounts posted links to websites that promised to inform protesters about the demonstration if they downloaded a smartphone app. The app included Finspy software and allowed the government to gain real-time access to the smartphone owners contacts, photos and videos.			SOU_0036	EVE_TAR_0126
EVE_0030	First known US target of cyberespionage in Europe. A U. S. and Greek national who worked on Meta's security and trust team while based in Greece was placed under a yearlong wiretap by the Greek national intelligence service and hacked with a cyberespionage tool, according to documents obtained by The New York Times	TAR_0132	Artemis Seaford	Individual	Other	Manager	Phishing	The target was placed under a yearlong wiretap by the Greek national intelligence service and hacked with a powerful cyberespionage tool while working as a manager for Meta on cybersecurity policies for which she we was in contact with several European officials. She was partly living in Greece an the US. The simultaneous tapping of the target's phone by the national intelligence service and the way she was hacked indicate that the spy service and whoever implanted the spyware, known as Predator, were working hand in hand.	Two people with direct knowledge of the case said that Ms. Seaford had in fact been wiretapped by the Greek spy service from August 2021, the month before the spyware hack, and for several months into 2022. fourth known person to file suit in Greece involving the spyware, after an investigative reporter and two opposition politicians.		SOU_0038	EVE_TAR_0127

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0031	Ethiopian dissidents in the US, UK, and other countries were targeted with emails containing sophisticated commercial spyware posing as Adobe Flash updates and PDF plugins. Targets include a US-based Ethiopian diaspora media outlet, the Oromia Media Network (OMN), a PhD student, and a lawyer. During the course of Citizen Lab's investigation, one of the authors of their report was also targeted.	TAR_0141	Jawar Mohammed	Individual	Advocacy	Executive Director	Phishing	Jawar is a prolific activist, with more than 1.2 million followers on Facebook. He was active on social media during a stampede in 2016 at the Oromo cultural festival, triggered by security forces use of teargas and discharge of firearms. On October 4, 2016, while in Minneapolis, USA, Jawar received the email which would have lead to an infection. He forwarded the email to Citizen Lab for analysis. In all, Jawar received eleven emails between 5/30/2016 and 10/13/2016, and one more than a year later on 11/22/2017. The Ethiopian Government charged Jawar with terrorism in February 2017 under the criminal code; Jawar and OMN denied all charges.			SOU_0040	EVE_TAR_0128
EVE_0031	Ethiopian dissidents in the US, UK, and other countries were targeted with emails containing sophisticated commercial spyware posing as Adobe Flash updates and PDF plugins. Targets include a US-based Ethiopian diaspora media outlet, the Oromia Media Network (OMN), a PhD student, and a lawyer. During the course of Citizen Lab's investigation, one of the authors of their report was also targeted.	TAR_0142	Oromia Media Network (OMN)	Other	Media	Media channel	Phishing	N/a			SOU_0040	EVE_TAR_0129
EVE_0031	Ethiopian dissidents in the US, UK, and other countries were targeted with emails containing sophisticated commercial spyware posing as Adobe Flash updates and PDF plugins. Targets include a US-based Ethiopian diaspora media outlet, the Oromia Media Network (OMN), a PhD student, and a lawyer. During the course of Citizen Lab's investigation, one of the authors of their report was also targeted.	TAR_0143	Etana Habte	Individual	Educatiion	Phd candidate	Phishing	Etana received two malicious emails on 12/9/2016 and on 1/11/2017. one of the emails came from the address shigut.gelleta@gmail.com appears to be an account created by attackers designed to impersonate Shigut Geleta, a member of the OLF.			SOU_0040	EVE_TAR_0130
EVE_0031	Ethiopian dissidents in the US, UK, and other countries were targeted with emails containing sophisticated commercial spyware posing as Adobe Flash updates and PDF plugins. Targets include a US-based Ethiopian diaspora media outlet, the Oromia Media Network (OMN), a PhD student, and a lawyer. During the course of Citizen Lab's investigation, one of the authors of their report was also targeted.	TAR_0144	Dr. Henok Gabisa	Individual	Educatiion	Visiting Academic Fellow	Phishing	Henok also received two malicious emails on 3/6/2017 and on 3/13/2017. Both came from the address networkoromostudies2015			SOU_0040	EVE_TAR_0131
EVE_0031	Ethiopian dissidents in the US, UK, and other countries were targeted with emails containing sophisticated commercial spyware posing as Adobe Flash updates and PDF plugins. Targets include a US-based Ethiopian diaspora media outlet, the Oromia Media Network (OMN), a PhD student, and a lawyer. During the course of Citizen Lab's investigation, one of the authors of their report was also targeted.	TAR_0145	Bill Marczak	Individual	Advocacy	Researcher	Phishing	Marczak was targeted after he asked another target to forward an email sent by operators. At the time, the target's email account was compromised (the target had been previously infected with this spyware). On March 29, 2017, while in San Francisco, USA, Marczak received a message entitled "Martin Plaut and Ethiopia's politics of famine," from networkoromostudies2015[@]gmail.com. The email contained a link to eastafro[.]net.			SOU_0040	EVE_TAR_0132
EVE_0029	The spyware attacked 12 people from Armenia after a series of clashes along the Armenia-Azerbaijan border in 2021, right after the violence that erupted in the Nagorno-Karabakh region in 2020.	TAR_0128	Anna Naghdalyan	Individual	Advocacy	Currently an NGO worker. Anna was officially serving as the Spokesperson of the Ministry of Foreign Affairs (MFA) of the Republic of Armenia during the time of the attack.	Unknown	Her phone was hacked at least 27 times between October 2020 and July 2021, with infections happening almost every single month. The attacks happened while she was serving as the Spokesperson for the MFA and had access to sensitive information about the Nagorno-Karabakh crisis on her phone. She expressed that there is no way for her to feel fully secured as her phone was infected with pegasus.			SOU_0039	EVE_TAR_0133
EVE_0029	The spyware attacked 12 people from Armenia after a series of clashes along the Armenia-Azerbaijan border in 2021, right after the violence that erupted in the Nagorno-Karabakh region in 2020.	TAR_0129	Karlen Aslanyan	Individual	Media	Radio Journalist	Unknown	Karlen was attacked when he was covereing the Armenian political crisis that had its roots in Armenia's defea			SOU_0039	EVE_TAR_0134
EVE_0029	The spyware attacked 12 people from Armenia after a series of clashes along the Armenia-Azerbaijan border in 2021, right after the violence that erupted in the Nagorno-Karabakh region in 2020.	TAR_0130	Kristinne Grigoryan	Individual	Humanitarian	Kristinne was serving as the Human Rights Ombudsperson (defender) for the Republic of Armenia when she was attacked.	Unknown	Kristinne was serving as the Human Rights Ombudsperson when her phone was infected. She was vocal about the atrocities committed against Armenian soldiers by Azerbaijani forces and was actively involved in publishing fact-finding and analytical reports, presenting evidence, and briefing diplomats in Armenia and international media. Due to this the Azerbaijan govt accused her of acting as a "foreign policy instrument."			SOU_0039	EVE_TAR_0135
EVE_0029	The spyware attacked 12 people from Armenia after a series of clashes along the Armenia-Azerbaijan border in 2021, right after the violence that erupted in the Nagorno-Karabakh region in 2020.	TAR_0131	Astghik Bedevyan	Individual	Media	Senior Journalist	Unknown	Astghik's device was infected in the month leading up to the Armenian parliamentary elections. Her phone c			SOU_0039	EVE_TAR_0136
EVE_0029	The spyware attacked 12 people from Armenia after a series of clashes along the Armenia-Azerbaijan border in 2021, right after the violence that erupted in the Nagorno-Karabakh region in 2020.	TAR_0133	Ruben Melikyan	Individual	Advocacy	Founder of Path of Law (NGO)	Unknown	Ruben has been one of the most outspoken critics of the Armenian government, both on external and interr			SOU_0039	EVE_TAR_0137
EVE_0029	The spyware attacked 12 people from Armenia after a series of clashes along the Armenia-Azerbaijan border in 2021, right after the violence that erupted in the Nagorno-Karabakh region in 2020.	TAR_0134	Dr. Varuzhan Geghamyan	Individual	Educatiion	Assistant Professor at the Yerevan State University, Turkologist, and a lecturer on the issue of regional and external politics of Azerbaijan	Unknown	During the time Dr. Varuzhan's phone was infected, he was regularly delivering public lectures before differe			SOU_0039	EVE_TAR_0138

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0029	The spyware attacked 12 people from Armenia after a series of clashes along the Armenia-Azerbaijan border in 2021, right after the violence that erupted in the Nagorno-Karabakh region in 2020.	TAR_0135	Samvel Farmanyan	Individual	Media	ArmNews TV co-founder	Unknown	Samvel had criticized the Armenian government following its defeat in the 2020 Nagorno-Karabakh War. His channel shut in February 2022 and his phone was infected around June 2022.			SOU_0039	EVE_TAR_0139
EVE_0029	The spyware attacked 12 people from Armenia after a series of clashes along the Armenia-Azerbaijan border in 2021, right after the violence that erupted in the Nagorno-Karabakh region in 2020.	TAR_0136	Anonymous	Individual	Media	Media representative	Unknown	They received Apple's notification about their phone being infected with Pegasus.			SOU_0039	EVE_TAR_0140
EVE_0029	The spyware attacked 12 people from Armenia after a series of clashes along the Armenia-Azerbaijan border in 2021, right after the violence that erupted in the Nagorno-Karabakh region in 2020.	TAR_0137	Anonymous	Individual	Media	Media representative	Unknown	They received Apple's notification about their phone being infected with Pegasus.			SOU_0039	EVE_TAR_0141
EVE_0029	The spyware attacked 12 people from Armenia after a series of clashes along the Armenia-Azerbaijan border in 2021, right after the violence that erupted in the Nagorno-Karabakh region in 2020.	TAR_0138	Anonymous	Individual	Advocacy	Activist	Unknown	They received Apple's notification about their phone being infected with Pegasus.			SOU_0039	EVE_TAR_0142
EVE_0029	The spyware attacked 12 people from Armenia after a series of clashes along the Armenia-Azerbaijan border in 2021, right after the violence that erupted in the Nagorno-Karabakh region in 2020.	TAR_0139	Anonymous	Individual	Advocacy	Armenian civil society actor	Unknown	They received Apple's notification about their phone being infected with Pegasus.			SOU_0039	EVE_TAR_0143
EVE_0029	The spyware attacked 12 people from Armenia after a series of clashes along the Armenia-Azerbaijan border in 2021, right after the violence that erupted in the Nagorno-Karabakh region in 2020.	TAR_0140	Anonymous	Individual	Humanitarian	United Nations representative	Unknown	They received Apple's notification about their phone being infected with Pegasus.			SOU_0039	EVE_TAR_0144
EVE_0032	Senior officials at EU Commission were targeted using ForcedEntry, an advanced piece of software that was used by Israeli cyber surveillance vendor NSO Group to help foreign spy agencies remotely and invisibly take control of iPhones.	TAR_0146	Didier Reynders	Individual	Politics	European Justice Commissioner since 2019	Zero-Click exploit	The commission became aware of the targeting following messages issued by Apple to thousands of iPhone owners in November telling them they were "targeted by state-sponsored attackers," the two EU officials said. It was the first time here Apple had sent a mass alert to users that they were in government hackers' crosshairs.			SOU_0041	EVE_TAR_0145
EVE_0033	An attacker made three separate attempts to target two Ethiopian Satellite Television Service (ESAT) employees with sophisticated computer spyware, designed to steal files and passwords, and intercept Skype calls and instant messages.	TAR_0147	Two ESAT employees	Individual	Media	Two workers of ESAT. Ethiopian Satellite Television Service (ESAT) is an independent satellite television, radio, and online news media outlet run by members of the Ethiopian diaspora.	Phishing	First, the ESATSTUDIO Skype account was targeted with spyware by receiving files to open. Remote Control System infects a target's computer or mobile phone to intercept data before it is encrypted for transmission, and can also intercept data that is never transmitted.			SOU_0042	EVE_TAR_0146
EVE_0034	Exodus spyware has infected hundreds of people for months thanks to several malicious Android apps that had been uploaded to Google's official Play Store. More than 20 malicious apps went unnoticed under Google's nose over a period of about two years.	TAR_0148	Hundreds of Italians	Individual	Other	Italian citizens	Zero-Click exploit	Exodus, distributed through Google Play Store, would have inadvertently downloaded the infected apps to Android devices.			SOU_0043	EVE_TAR_0147
EVE_0035	Carine Kanimba, daughter of Paul Rusesabagina, the imprisoned Rwandan activist who inspired the film Hotel Rwanda, has been the victim of a near-constant surveillance campaign.	TAR_0149	Carine Kanimba	Individual	Advocacy	Daughter of Paul Rusesabagina, the imprisoned Rwandan activist who inspired the film Hotel Rwanda. She has been advocating for release of her father.	Zero-Click exploit	Kanimba's phone had been infiltrated with Pegasus, giving access to her phone calls and messages, and turning the mobile phone into a portable tracking and listening device.			SOU_0044	EVE_TAR_0148
EVE_0036	Kamel Jendoubi, a Tunisian who served as the chairman of the now defunct Group of Eminent Experts in Yemen (GEE)– a panel mandated by the UN to investigate possible war crimes – was targeted in August 2019.	TAR_0150	Kamel Jendoubi	International Organization	Legal	Chairman of the now defunct UN Group of Eminent Experts in Yemen (GEE)	Zero-Click exploit	Jendoubi's phone was infected just weeks before Jendoubi and his panel of experts released a damning report which concluded that the Saudi-led coalition in the Yemen war had committed "serious violations of international humanitarian law" that could lead to "criminal responsibility for war crimes".			SOU_0045	EVE_TAR_0149
EVE_0037	Spanish Prime Minister Pedro Sánchez and Defense Minister Margarita Robles were targeted with Pegasus spyware that surveilled their mobile phones	TAR_0151	Pedro Sánchez	Individual	Politics	Spanish Prime Minister	Zero-Click exploit	Phones have been infected twice and large amounts of data were extracted from both phones, the government said.			SOU_0046	EVE_TAR_0150
EVE_0037	Spanish Prime Minister Pedro Sánchez and Defense Minister Margarita Robles were targeted with Pegasus spyware that surveilled their mobile phones	TAR_0152	Margarita Robles	Individual	Politics	Spanish Defense Minister	Zero-Click exploit	Phones have been infected twice and large amounts of data were extracted from both phones, the government said.			SOU_0046	EVE_TAR_0151
EVE_0038	Greek intelligence services, as well as the use of spyware, targeting MEP Nikos Androulakis , the leader of the Greek opposition party PASOK-KINAL.	TAR_0153	Nikos Androulakis	Political Party/Organization	Politics	MEP and leader of the Greek opposition party PASOK-KINAL	Phishing	Androulakis was informed that he had been the victim of an unsuccessful wiretapping attempt through the use of Predator software. Predator spyware can circumvent encryption of internet communication services and directly exfiltrate communication data processed by the target system. Predator requires its targets to open a link in order to infiltrate their devices.			SOU_0047	EVE_TAR_0152
EVE_0039	The mobile phone of François de Rugy, who was environment minister at the time of the activity, showed digital traces of activity associated with Pegasus. In total, 14 serving members of the French government appear in a leaked list of potential targets.	TAR_0154	François de Rugy	Individual	Politics	Environment minister at the time of the activity	Zero-Click exploit	The forensic analysis on De Rugy's phone was undertaken by Amnesty International's Security Lab. It showed traces of a Pegasus-related activity on the device, but no evidence of a successful infection.		Refer to section EventProfile for context on the case	SOU_0048	EVE_TAR_0153
EVE_0040	The phones of two French journalists were bugged with the Pegasus spyware, an investigation by France's national cybersecurity agency found.	TAR_0155	Lenaig Bredoux	Individual	Media	Journalist	Zero-Click exploit	Numbers were part of the leaked database of 50,000 mobile phone numbers of the NSO Group. Evidence of Pegasus was found on the phones.		For more context refer to SOU_0048	SOU_0049	EVE_TAR_0154
EVE_0040	The phones of two French journalists were bugged with the Pegasus spyware, an investigation by France's national cybersecurity agency found.	TAR_0156	Edwy Plenel	Individual	Media	Journalist	Zero-Click exploit	Numbers were part of the leaked database of 50,000 mobile phone numbers of the NSO Group. Evidence of Pegasus was found on the phones.		For more context refer to SOU_0048	SOU_0049	EVE_TAR_0155

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0041	A British human rights campaigner and lawyer who was fighting to free Dubai's Princess Latifa had his mobile phone compromised by Pegasus spyware	TAR_0157	David Haigh	Individual	Advocacy	Human rights campaigner and lawyer	Zero-Click exploit	Amnesty's analysis of Haigh's phone concluded there was evidence of a Pegasus-related infection via Apple's iMessage. It is not clear what impact this had in this case, however.			SOU_0050	EVE_TAR_0156
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0158	Roger Torrent	Individual	Politics	Pro-independence Former president of the Catalan Parliament	Unknown	The targeting of Torrent with Pegasus spyware was confirmed by WhatsApp.			SOU_0051	EVE_TAR_0157
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0159	Ernest Maragall	Individual	Politics	Leader of the pro-independence Republican Left of Catalonia party	Unknown	Targeting with Pegasus through Whatsapp			SOU_0051	EVE_TAR_0158
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0160	Anna Gabriel	Individual	Politics	Former regional member of Parliament for the far-left party, the Popular Unity Candidacy (CUP)	Unknown	Targeting with Pegasus through Whatsapp			SOU_0051	EVE_TAR_0159
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0161	Diana Riba	Individual	Politics	Catalan MEP	Unknown	Targeting with Pegasus through Whatsapp			SOU_0051	EVE_TAR_0160
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0162	Jordi Solé	Individual	Politics	Catalan MEP	Phishing	Targeted with Pegasus during party discussions about who would replace MEP Oriol Junqueras. One instance took the form of a fake SMS from Spain's social security system. Forensic evidence confirms that he was infected at least twice on or around June 11 and June 27, 2020, shortly before being substituted into his role as a MEP in July 2020.			SOU_0051	EVE_TAR_0161
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0163	Pol Cruz	Individual	Politics	Parliamentary staff member	Unknown	Infected with Pegasus in July 2020			SOU_0051	EVE_TAR_0162
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0164	Jordi Domingo	Individual	Politics	Activist	Unknown	Infected with Pegasus			SOU_0051	EVE_TAR_0163
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0165	Sergi Miquel Gutiérrez	Individual	Politics	Staffer of Puigdemont, 2016-2017 President of Catalonia	Unknown	Infected with Pegasus			SOU_0051	EVE_TAR_0164
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0166	Marcela Topor	Individual	Other	Spouse of Puigdemont	Unknown	Infected multiple times with Pegasus			SOU_0051	EVE_TAR_0165
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0167	Jordi Sànchez	Individual	Politics	Board Member and 2015-2017 President of ANC	Phishing	Sànchez was first seen targeted with a Pegasus SMS infection attempt via SMS 2015, shortly after a large demonstration in Barcelona. This is the earliest Pegasus infection attempt that we have observed as bulk of the targeting uncovered by this investigation appears to have occurred between 2017 and 2020. Between 2017 and 2020, Sànchez received at least 24 more Pegasus SMSes, most of which masqueraded as news updates relating to Catalan and Spanish politics. He also received messages purporting to come from the Spanish tax and social security authorities.			SOU_0051	EVE_TAR_0166
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0168	Elisenda Paluzie	Individual	Politics	ANC President, 2018-2022	Phishing	Infected with Pegasus			SOU_0051	EVE_TAR_0167

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0169	Sònia Urpí Garcia	Individual	Politics	ANC board member	Phishing	Infected with Pegasus			SOU_0051	EVE_TAR_0168
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0170	Meritxell Bonet	Individual	Media	Journalist and spouse of Òmnium's former president Jordi Cuixart	Unknown	Infected with Pegasus			SOU_0051	EVE_TAR_0169
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0171	Marcel Mauri	Individual	Advocacy	Vice president of Òmnium after Cuixart in 2019	Phishing	Within ten days of assuming the role, on October 24, 2019, evidence of what would be the first of three Pegasus infections of his phone. Also found evidence of extensive Pegasus SMS targeting straddling that period, beginning in February 2018 and ending in May 2020.			SOU_0051	EVE_TAR_0170
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0172	Elena Jiménez	Individual	Advocacy	Executive board member	Unknown	Infected with Pegasus. Her role included dialogue with NGOs throughout Europe including Amnesty International and Frontline Defenders. The compromise of her communications would have likely provided a unique view into Catalan advocacy efforts.			SOU_0051	EVE_TAR_0171
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0173	Jordi Bosch	Individual	Advocacy	Executive board member	Unknown	Infected with Pegasus			SOU_0051	EVE_TAR_0172
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0174	Joan Matamala	Individual	Advocacy	Founder of Nord Foundation which promotes open-source citizen participation software	Unknown	Forensic examination of his phone indicates that he was also infected at least 16 times with Pegasus and Candiru between August 2019 and July 2020.			SOU_0051	EVE_TAR_0173
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0175	Gonzalo Boye	Individual	Legal	Lawyer	Phishing	Was targeted at least 18 times with Candiru infection attempts between January and May 2020. Some of the messages masqueraded as tweets from organisations like Human Rights Watch, The Guardian, Columbia Journalism Review, and Politico. Boye was successfully infected with Pegasus on or around October 30, 2020.			SOU_0051	EVE_TAR_0174
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0176	Andreu Van den Eynde	Individual	Legal	Lawyer	Phishing	Infected with Pegasus and Candiru			SOU_0051	EVE_TAR_0175
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0177	Pere Aragonès	Individual	Politics	Catalan president, 2021-present	Unknown	Infected with Pegasus			SOU_0051	EVE_TAR_0176
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0178	Joaquim Torra	Individual	Politics	Catalan president, 2018-2020	Unknown	Infected with Pegasus			SOU_0051	EVE_TAR_0177
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0179	Carles Puigdemont	Individual	Politics	Catalan president, 2016-2017	Unknown	Infected with Pegasus			SOU_0051	EVE_TAR_0178
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0180	Artur Mas	Individual	Politics	Catalan president, 2010-2015	Unknown	Infected with Pegasus			SOU_0051	EVE_TAR_0179

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0181	Laura Borràs	Individual	Politics	Current President of Catalan parliament	Unknown	Infected with Pegasus			SOU_0051	EVE_TAR_0180
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0182	11 Members	Political Party/Organization	Politics	Members of political party Together for Catalonia	Unknown	Infected with Pegasus			SOU_0051	EVE_TAR_0181
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0183	12 Members	Political Party/Organization	Politics	Members of political party Republican Left of Catalonia	Unknown	Infected with Pegasus			SOU_0051	EVE_TAR_0182
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0184	4 Members	Political Party/Organization	Politics	Members of political party Popular Unity Candidacy	Unknown	Infected with Pegasus			SOU_0051	EVE_TAR_0183
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0185	3 Members	Political Party/Organization	Politics	Members of political party Catalan European Democratic Party	Unknown	Infected with Pegasus			SOU_0051	EVE_TAR_0184
EVE_0042	The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware. Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.	TAR_0186	1 Members	Political Party/Organization	Politics	Member of political party Catalan Nationalist Party	Unknown	Infected with Pegasus			SOU_0051	EVE_TAR_0185
EVE_0043	Nine Bahraini Activists' iPhones were hacked by Pegasus as identified by Citizen Lab.	TAR_0187	Moosa Abd-Ali	Individual	Advocacy	Activist	Zero-Click exploit	He has been living in exile in London, UK. Abd-Ali's iPhone 8 was hacked with Pegasus in September 2020. He had sued FinFisher in 2011, for supplying the Bahraini government with spyware that was used to hack his personal computer.			SOU_0052	EVE_TAR_0186
EVE_0043	Nine Bahraini Activists' iPhones were hacked by Pegasus as identified by Citizen Lab.	TAR_0188	Yusuf Al-Jamri	Individual	Media	Blogger	Zero-Click exploit	He was granted asylum by the UK Government in 2018, as he was tortured by the Bahraini Intelligence Agency in 2017. His device was infected with Pegasus, but it isn't sure if he was hacked in London or Bahrain.			SOU_0052	EVE_TAR_0187
EVE_0043	Nine Bahraini Activists' iPhones were hacked by Pegasus as identified by Citizen Lab.	TAR_0189	Anonymous	Individual	Advocacy	Member	Zero-Click exploit	Infected with Pegasus			SOU_0052	EVE_TAR_0188
EVE_0043	Nine Bahraini Activists' iPhones were hacked by Pegasus as identified by Citizen Lab.	TAR_0190	Anonymous	Individual	Advocacy	Member	Zero-Click exploit	Infected with Pegasus			SOU_0052	EVE_TAR_0189
EVE_0043	Nine Bahraini Activists' iPhones were hacked by Pegasus as identified by Citizen Lab.	TAR_0191	Anonymous	Individual	Advocacy	Member	Zero-Click exploit	Infected with Pegasus			SOU_0052	EVE_TAR_0190
EVE_0043	Nine Bahraini Activists' iPhones were hacked by Pegasus as identified by Citizen Lab.	TAR_0192	Anonymous	Individual	Advocacy	Member	Zero-Click exploit	Infected with Pegasus			SOU_0052	EVE_TAR_0191
EVE_0043	Nine Bahraini Activists' iPhones were hacked by Pegasus as identified by Citizen Lab.	TAR_0193	Anonymous	Individual	Advocacy	Member	Zero-Click exploit	Infected with Pegasus			SOU_0052	EVE_TAR_0192
EVE_0043	Nine Bahraini Activists' iPhones were hacked by Pegasus as identified by Citizen Lab.	TAR_0194	Anonymous	Individual	Advocacy	Member	Zero-Click exploit	Infected with Pegasus			SOU_0052	EVE_TAR_0193
EVE_0043	Nine Bahraini Activists' iPhones were hacked by Pegasus as identified by Citizen Lab.	TAR_0195	Anonymous	Individual	Politics	Member	Zero-Click exploit	Infected with Pegasus			SOU_0052	EVE_TAR_0194
EVE_0044	Lama Fakih, Human Rights Watch's Middle East and North Africa Division Director and Beirut office Head, was targeted with Pegasus spyware at least five times between April and August 2021	TAR_0196	Lama Fakih	Individual	Advocacy	Middle East and North Africa Division Director	Zero-Click exploit	Her phone was attacked on the day she was celebrating her child's first birthday. In The Washington Post opinio piece, she expressed that it was "paralyzing and chilling" for her to experience the unlawful surveillance. One of the reasons for the attack could be attributed to her being the director of the Human Rights Watch Crisis and Conflict Division during that time.			SOU_0053	EVE_TAR_0195

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0045	A prominent scientist at the Mexican National Institute for Public Health (INSP) and two directors of Mexican NGOs working on obesity and soda consumption were targeted with government-exclusive spyware.	TAR_0197	Simón Barquera	Individual	Educatiion	Researcher	Phishing	Simón Barquera (that we know of) began with the operators sending him a message on July 11, 2016 with a fake news story relevant to his work. The Bitter Sweet operators subsequently escalated the personal content and aggressiveness of the messages in two waves, ending on August 17. The repeated messages and escalation of emotional content suggest a strong desire on the part of the operators to compromise Dr. Barquera's device. The Bitter Sweet operators may have either failed to infect Dr. Barquera's devices with NSO's Pegasus or had trouble maintaining a stable infection on the target device	Campaigners held a press conference on June 29, 2016, highlighting misleading and confusing product labelling standards promoted by the food and beverage industry and planned a full launch of their campaign in August 2016. Campaigners began receiving the spyware links one week after the press conference, and throughout the period that the campaign was being prepared	The same infrastructure used for the Bitter Sweet operation (the unonoticias[.]net domain) was also used to target a Mexican journalist who wrote a story about government corruption involving the Mexican President's wife and a high-speed rail contractor, among other domestic targeting.	SOU_0054	EVE_TAR_0196
EVE_0045	A prominent scientist at the Mexican National Institute for Public Health (INSP) and two directors of Mexican NGOs working on obesity and soda consumption were targeted with government-exclusive spyware.	TAR_0198	Alejandro Calvillo	Individual	Advocacy	Director	Phishing	Alejandro Calvillo also received a message about a father's funeral on July 8 and a message on July 11 stating that his name was mentioned in a news article that was "going viral."	The messages sent all contained links pointing to domains previously identified as part of our investigation into NSO's infrastructure. The URLs in several text messages directly linked to the exploit infrastructur		SOU_0054	EVE_TAR_0197
EVE_0045	A prominent scientist at the Mexican National Institute for Public Health (INSP) and two directors of Mexican NGOs working on obesity and soda consumption were targeted with government-exclusive spyware.	TAR_0199	Luis Encarnación	Individual	Advocacy	Coordinator	Phishing	Luis Encarnación, meanwhile, received a message on July 12 suggesting that he was mentioned in a news article			SOU_0054	EVE_TAR_0198
EVE_0046	the journalist Rafael Cabrera, who recently reported on the Casa Blanca controversy, a reported conflict of interest involving the President and First Lady of Mexico reiceived phishing messages	TAR_0200	Rafael Cabrera	Individual	Media	Journalist	Phishing	the journalist received multiple phishing messges which got increasingly desparate (the last containing profane and personal sexual taunts, unlike the other messages). Citizen lab believes that each of these messages contained a link that would have led to the infection of his iPhone with NSO Group's Pegasus spyware via the Trident exploit.	Similar SMS messages have also been reported in other online posts from Mexico.		SOU_0008	EVE_TAR_0199
EVE_0047	A tweet containing a link to the NSO Group infrastructure targeting the minority leader in Kenya's senate.	TAR_0201	Moses Wetangula	Individual	Politics	Politician	Phishing	A tweet by a person who proclaims to be a senior research officer contained a link to a pegasus infection. it was directed at the former minority leader in the senate. There is no impact recorded as the tweet was discovered directly by citizen lab		this was only an attempt through a tweet discovered by citizen lab directly	SOU_0008	EVE_TAR_0200
EVE_0048	3 Togolese journalists were reported as potential spyware targets through the Pegasus project	TAR_0202	Komlanvi Ketohou	Individual	Media	Journalist	Phishing	He fled Togo in early 2021 and left behind his his cell phone that the gendarmerie seized when they arrested and detained him over a report published by his newspaper, L'Independant Express. In July, Ketohou, who goes by Carlos, learned that the phone number connected to the device they took may have been targeted for surveillance years before his arrest: "I spent nightmarish nights thinking about all my phone activities. My private life, my personal problems in the hands of strangers," Ketohou said. "It's scary. And it's torture for me." e said it confirmed his decision to go into exile, where he started a new news site, L' Express International, after Togo's media regulator barred L'Independant Express from publishing in early 2021 as CPJ documented.	The three journalists told CPJ in multiple interviews conducted via email, phone, and messaging app that learning of their status as potential surveillance targets heightened their sense of insecurity, even as they continue to work in the profession.	not confirmed, they are just part of the list of potential targets	SOU_0055	EVE_TAR_0201
EVE_0048	3 Togolese journalists were reported as potential spyware targets through the Pegasus project	TAR_0203	Ferdinand Ayité	Individual	Media	Journalist	Phishing	"There is a huge psychological impact of knowing that someone in this country is taking control of your phone, violating your privacy," Ayité told CPJ, adding that his broader safety and privacy concerns had already caused him to limit his dating and other personal relationships. "I will be even more careful and vigilant you never know where the fatal blow will come from. I am a journalist on borrowed time."			SOU_0055	EVE_TAR_0202
EVE_0048	3 Togolese journalists were reported as potential spyware targets through the Pegasus project	TAR_0204	Luc Abaki	Individual	Media	Journalist	Phishing	Abaki said that being listed for surveillance was "extremely traumatic," adding "there is no private life." "I told myself that I could have died, since the other journalists targeted from the other countries were murdered," Ketohou told CPJ.			SOU_0055	EVE_TAR_0203
EVE_0049	NSO spyware was used in 2019 to target Togolese civil society, including a Catholic bishop, priest, and opposition politicians.	TAR_0205	Benoît Comlan Alowonou	Individual	Community/Spiritual/Faith-Based	Bishop of Kpalimé	Phishing	The targeting in April – May 2019 coincided with nationwide protests calling for presidential term limits. Planned demonstrations by the opposition Pan-African National Party (PNP) were largely banned by the government, which only permitted demonstrations in three cities. On April 13, 2019, protestors were violently dispersed by armed security forces, with one person killed and many others injured. Dozens of journalists, opposition leaders, and human rights defenders were detained. Detained in inhumane conditions, 19 were later sentenced to prison.	The Bishop has been the target of misinformation, and false reporting. During a visit with the Pope, he recognized the Togolese Bishops for their efforts for justice, peace and reconciliation, while cautioning about political entanglements. According to the Diocese, while the Bishop was in Rome it was falsely reported by a Togolese outlet that he had called on the opposition to "admit electoral defeat."	In our 2018 Hide and Seek report, Citizen Lab identified a single Pegasus operator spying in Togo that we called REDLIONS. Because the operator appeared to be spying only in Togo, we suspected that REDLIONS was operated by an agency of the Togolese Government.	SOU_0056	EVE_TAR_0204

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0049	NSO spyware was used in 2019 to target Togolese civil society, including a Catholic bishop, priest, and opposition politicians.	TAR_0206	Father Pierre Marie-Chanel Affognon	Individual	Community/Spiritual/Faith-Based	Priest	Phishing	same as above	In 2018 and into 2019, Father Affognon was the target of a smear and disinformation campaign apparently intended to undermine his activities and those of the movement. Father Affognon speculates that the authors of this campaign may have had access to personal information only available on his phone.		SOU_0056	EVE_TAR_0205
EVE_0049	NSO spyware was used in 2019 to target Togolese civil society, including a Catholic bishop, priest, and opposition politicians.	TAR_0207	Elliott Ohin	Individual	Politics	Politician	Phishing	same as above			SOU_0056	EVE_TAR_0206
EVE_0049	NSO spyware was used in 2019 to target Togolese civil society, including a Catholic bishop, priest, and opposition politicians.	TAR_0208	Raymond Houndjo	Individual	Politics	Politician	Phishing	same as above			SOU_0056	EVE_TAR_0207
EVE_0050	WhatsApp in collaboration with CitizenLab reached out to this target as they found an attempt to attack the targets phone.	TAR_0209	Placide Kayumba	Individual	Politics	Activist and Politician	Phishing	CitizenLab contacted the person to ask the questions regarding abnormalities on their phone because they saw an attempt to attack their phone. Later Whatsapp confirmed that his phone was targeted.			SOU_0057	EVE_TAR_0208
EVE_0017	Phones of Palestinian activists working for the human rights NGOs were hacked.	TAR_0210	Ghassan Halaika	Individual	Advocacy	Human Rights Defender	Zero-Click exploit	"There were some bizarre things happening on my phone such as people receiving calls from me which I hadn't made". As a result of his concerns, Al Haq asked Front Line Defenders, an Irish-based human rights organisation, to investigate the matter. This lead to the discovery that in addition to Halaika's phone, which had been under surveillance since June 2020, at least five other phones belonging to employees of the six organisations and other rights activists had been infected with Pegasus spyware. "I never thought that things could go this far," "Can you imagine how you would feel if you knew that your every movement and telephone conversation was being monitored by unknown people, that your safety was compromised and that you had no privacy?"	"I'm trying to continue my work as normal but it's not easy," said Halaika. "What really hurts is that confidential information I had worked on with private contacts, in regard to pursuing Israeli war crimes at the International Criminal Court, was uncovered during the surveillance and has hurt some of my contacts."		SOU_0058; SOU_0059; SOU_0060	EVE_TAR_0209
EVE_0017	Phones of Palestinian activists working for the human rights NGOs were hacked.	TAR_0211	T4	Individual	Advocacy	Human Rights Defender	Zero-Click exploit	Phone infected on 2021-04-12		some dates of hacking may not be particularly significant, as zero-click hacking can sometimes be driven by availability of exploits rather than specific timeframes of interest.	SOU_0058; SOU_0059; SOU_0060	EVE_TAR_0210
EVE_0017	Phones of Palestinian activists working for the human rights NGOs were hacked.	TAR_0212	T5	Individual	Advocacy	Human Rights Defender	Zero-Click exploit	Phone infected on 2021-02-10, 2021-04-03, 2021-04-12			SOU_0058; SOU_0059; SOU_0060	EVE_TAR_0211
EVE_0017	Phones of Palestinian activists working for the human rights NGOs were hacked.	TAR_0213	T6	Individual	Advocacy	Human Rights Defender	Zero-Click exploit	Phone infected on 2020-11-04			SOU_0058; SOU_0059; SOU_0060	EVE_TAR_0212
EVE_0051	A prominent Western Sahara human rights activist in Morocco has been targeted with NSO Group's Pegasus spyware, just months after the Pegasus Project revelations	TAR_0214	Aminatou Haidar	Individual	Advocacy	Human Rights Defender	Zero-Click exploit	After receiving security alerts by email from Apple saying her phones may have been targeted by state-sponsored attackers, Aminatou Haidar contacted the Right Livelihood Foundation, who referred her to Amnesty International's Security Lab for forensic analysis. The Security Lab then confirmed the targeting and infection with NSO Group's Pegasus spyware. Amnesty International's analysis showed that one of Haidar's phones contained traces of Pegasus targeting dating back to September 2018, and further traces of infection as recently as October and November 2021 on the other. Amnesty International shared forensic records from Haidar's phone with Citizen Lab researchers at the University of Toronto, who independently confirmed the Pegasus infections from October and November 2021.	Danna Ingleton, Deputy Director of Amnesty Tech. "This latest revelation shows NSO Group's human rights policies are meaningless in practice. Amnesty International has repeatedly shown forensic evidence of Pegasus misuse since 2019 in Morocco, as well as in over a dozen countries in the Pegasus Project investigation, yet NSO Group has taken no action to prevent the ongoing human rights violations caused by its tools in Morocco.		SOU_0061	EVE_TAR_0213
EVE_0052	Phones belonging to four Jordanian human rights defenders, lawyers, and journalists were hacked with NSO Group's Pegasus spyware	TAR_0215	Ahmed Al-Neimat	Individual	Advocacy	Human Rights Defender, anti-corruption activist, and a member of the Hirak movement	Zero-Click exploit	Neimat has been arrested multiple times due to his activism and dissenting. His phone was hacked by pegasus in January 2021 for a period of two days, the same year he was arrested for protesting the release of another jailed Hirak activist.			SOU_0062	EVE_TAR_0214
EVE_0052	Phones belonging to four Jordanian human rights defenders, lawyers, and journalists were hacked with NSO Group's Pegasus spyware	TAR_0216	Malik Abu Orabi	Individual	Legal	Human Rights Lawyer and Member of the National Forum for the Defense of Liberties	Zero-Click exploit	Orabi's phone was hacked by pegasus at least 21 times between August 2019 and July 2021. He was also arrested for protesting in March 2021.			SOU_0062	EVE_TAR_0215
EVE_0052	Phones belonging to four Jordanian human rights defenders, lawyers, and journalists were hacked with NSO Group's Pegasus spyware	TAR_0217	Suhair Jaradat	Individual	Media	Journalist, Human rights defender and Advocate for women's issues in Media	Zero-Click exploit	Jaradat's iPhone was hacked six times between February and December 2021			SOU_0062	EVE_TAR_0216

EVE_ID	eventDescription	TAR_ID	targetName	targetType	targetPrimarySector	targetRole	attackVector	impactDescription	otherInformation	researcherNotes	SOU_ID	EVE_TAR_ID
EVE_0052	Phones belonging to four Jordanian human rights defenders, lawyers, and journalists were hacked with NSO Group's Pegasus spyware	TAR_0218	Anonymous	Individual	Media	Woman Human Rights Defender (WHRD) and Journalist	Zero-Click exploit	Her phone was hacked at least twice in October 2021. She asked to remain anonymous due to the risks she faces.			SOU_0062	EVE_TAR_0217
EVE_0053	Hacking of Women's human rights defender (WHRD) from Bahrain using Pegasus spyware	TAR_0219	Ebtisam El-Saegh	Individual	Advocacy	Human Rights Defender	Zero-Click exploit	Ebtisam El-Saegh's phone was hacked 8 times by pegasus. She claimed that she is "in a state of daily fear and terror" after knowing that her personal information was compromised. She is experiencing a form of paranoia with resoect to having her phone next to her and is scared of having her professional image tarnished due to the conservative society she's part of. The fear and anxiety have restricted her work and she does not want to put her family and colleagues at risk. She is afraid of leaving her house due to the fear of being unlawfully surveilled. The attack has affected her relations with people, as they are afraid of meeting her or getting in contact with her. She exclaimed- "Personal freedoms are over for me, they no longer exist. I am not safe at home, on the street, or anywhere."			SOU_0063	EVE_TAR_0218
EVE_0054	Hacking of Women's human rights defender (WHRD) from Jordan using Pegasus spyware	TAR_0220	Hala Ahed Deeb	Individual	Legal	Human Rights Lawyer	Zero-Click exploit	After being targeted by Pegasus, Hala Ahed Deeb expressed- "When your privacy is violated, you feel violated, naked, and with no dignity— this is how I feel." She expressed her fears of being a woman and losing her privacy in a conservative society. She feels isolated and is practising a form of self-censorship by avoiding communicating with people around her. She is experiencing a form of paranoia and is constantly wondering if she is being surveilled. Due to the hacking, she feels she has lost the space to express. She is also extremely worried about other victims, as she is working with multiple victims of human rights abuses.			SOU_0063	EVE_TAR_0219
EVE_0055	A Mexican investigative journalist received multiple SMS containing exploit links	TAR_0221	Carlos Loret de Mola	Individual	Media	Journalist & Moderator	Phishing	The NSO messages first arrived in August 2015 during a period when he was covering a massacre that took place on May 22, 2015 at a farm known as "Rancho El Sol" in western Mexico. On August 8, 2015, Loret published an article in which he claimed new evidence from the Mexican Federal Public Prosecutor's Office contradicted official claims at the time of the massacre, and showed Mexican security forces had actually committed extrajudicial killings. On August 20, 2015, Loret received SMS messages looking to be from the US Embassy involving issues with his visa application. He received further messges on August 29, September 1 and 6 and on March 5, 2016 and the last one on April 20.	similar text messages with details of a supposed "father's death" with links to NSO infrastructure were received on July 8, 2016 by Mexican health advocate Alejandro Calvillo, and on July 13, 2016 by the Mexican health scientist Dr. Simon Barquera. Similar to the other Mexican cases the messages included references to blackmail material (eg 'photos of you dining with a chick') and a father's death	connected to the other Mexican cases as part of the Citizen Lab reserach series on NSO in Mexico	SOU_0064	EVE_TAR_0220
EVE_0056	Two human rights defenders from Centro PRODH, which represents victims of military abuses in Mexico, were infected with an NSO Group exploit	TAR_0222	Jorge Santiago Aguirre Espinosa	Individual	Advocacy	Director	Zero-Click exploit	n 2022, he was infected at least twice via the FINDMYPWN exploit. The spyware was active on his device on June 22, 2022 and July 13, 2022. On June 22, 2022, the same date as the first infection of Mr. Aguirre's phone, Mexico's truth commission investigating the Dirty War launched its activities in a ceremony at a Mexican military camp where many of the abuses had taken place.	The September 2022 Pegasus attacks coincided with several events in the Ayotzinapa case, in which Centro PRODH represents the families of the disappeared. The attacks also coincide with the cancellation of several arrest warrants against military personnel involved in the Ayotzinapa case after pushback from the Mexican Army.	Ayotzinapa case is a reference to the Iguala mass kidnapping in September 2015 when a group of 43 students at a teacher training college were forcibly disappeared after traveling to Iguala to protest teacher hiring practices	SOU_0065	EVE_TAR_0221
EVE_0056	Two human rights defenders from Centro PRODH, which represents victims of military abuses in Mexico, were infected with an NSO Group exploit	TAR_0223	María Luisa Aguilar Rodríguez	Individual	Advocacy	International Coordinator	Zero-Click exploit	Maria was infected on June 23, 2022. Her work includes representing victims of human rights violations perpetrated by the Mexican army. She was subsequently infected twice more via the FINDMYPWN exploit. The spyware was active on her device on September 24, 2022 and September 29, 2022.	"FINDMYPWN" was deployed against iOS 15 beginning in June 2022. It appears to be a two-step exploit; the first step targets the iPhone's Find My feature, and the second step targets iMessage.		SOU_0065	EVE_TAR_0222
EVE_0057	Three human rights defenders of the Centro PRODH were infected with Pegasus while they represented the families of the forced disappeared 43 students.	TAR_0224	Mario Patrón	Individual	Advocacy	Director	Phishing	Received a phishing message with an exploit link on 4/20/2016 referencing a news about GIEI			SOU_0064; SOU_0066	EVE_TAR_0223
EVE_0057	Three human rights defenders of the Centro PRODH were infected with Pegasus while they represented the families of the forced disappeared 43 students.	TAR_0225	Stephanie Brewer	Individual	Advocacy	Staff	Phishing	Received a phishing message with an exploit link on 5/11/2016 referencing her human rights work			SOU_0064; SOU_0066	EVE_TAR_0224
EVE_0057	Three human rights defenders of the Centro PRODH were infected with Pegasus while they represented the families of the forced disappeared 43 students.	TAR_0226	Santiago Aguirre	Individual	Advocacy	Staff	Phishing	Received a phishing message with an exploit link on 5/20/2016 referencing a person seeking legal guidance. A recorded phone conversation between him and one parent was published in 2016 in a double blow to the families hoping for help from government. Aguirre said for the parents it was outrageous that technology whose stated aim was to catch criminals had been turned on victims, adding: "It makes you feel very vulnerable."			SOU_0064; SOU_0066	EVE_TAR_0225