Hertie School
Centre for
Digital Governance

Student Working Paper Series

Pegasus spyware in Europe

One year into the revelations of extensive spyware misuse —what has changed in the EU?

Johanna Pruessing, MPP 2022

10 October 2022

#Spyware

In July 2021, a collaborative civil society investigation called the 'Pegasus Project' triggered a series of revelations about instances of illegal spying carried out on journalists, lawyers, opposition figures and European heads of states by law enforcement agencies and other states. The present case study discusses state, corporate and civil society responses to the revelations and finds conflicting interests within governments and the tech industry over spyware regulation. This is the result of blind spots in digital governance as applied to the development, purchase, deployment, and oversight of commercially-developed, targeted spyware in Europe, which has paved the way for large-scale abuse. The case study concludes that security sector interests dominate the use of spyware. Governance in compliance with human rights would require a comprehensive reform effort on the side of governments to introduce effective accountability frameworks—for both the private and public sectors—for the trade and use of spyware.

Hertie School
Centre for
Digital Governance

Table of Contents

1 Introduction

In July 2021, a global collaborative investigative project involving 17 media organisations, alongside Amnesty International and Citizen Lab, revealed that the Israeli NSO Group's Pegasus spyware was being used to illegally spy on journalists, politicians, human rights defenders, lawyers and other critical voices around the world. Amnesty International and Forbidden Stories further acquired a leak with 50,000 phone numbers of possible Pegasus targets and following investigations confirmed that Pegasus had been used in Hungary, Poland, France, Spain and the UK (The Business and Human Rights Resource Centre, 2022). Among the targets were French President Emmanuel Macron and up to 15 ministers, Spanish Prime Minister Pedro Sánchez and Defence Minister Margarita Robles (Gijs, 2022), senior EU officials (Satter & Bing, 2022), president of the European Council Charles Michel (Matriche, 2021), representatives of Polish opposition groups (Bajak & Gera, 2021) Hungarian journalists (Bleyer-Simon, 2021), networks of the UK prime minister's office (Deibert, 2022), as well as around 65 individuals affiliated with the Catalan pro-independence movement (Scott-Railton et al., 2022).

Pegasus and similar tools have ostensibly been purchased by governments for the fight against terror and organised crime, but the revelations show that the software has also been used against political opponents, journalists and lawyers—violating human rights standards—and to undermine the European democratic order. These instances have made clear that Europe lacks effective regulation for the development and use of spyware such as Pegasus.

This case study takes stock of how government, corporations and civil society have responded to the Pegasus revelations in Europe since July 2021, highlighting governance factors that contributed to the abuses including challenges around documenting the spyware, conflicting interests within governments, lack of regulation of the private surveillance industry and the need for a victim-centred approach. The study concludes with the identification of possible areas for policy change.

2 Limited capacity to detect and document illegal spying

The governance of spyware faces one fundamental obstacle: Spyware, like Pegasus, is designed to be used in secret. Identifying who has been targeted by whom requires a high degree of financial resources and technical sophistication.

Pegasus can be remotely installed on a smartphone without a user's knowledge. NSO achieves this by exploiting unknown and thus unpatched flaws in the code - also known as "zero-click exploits" - or by using phishing techniques, making it hard, even for experts, to detect. Once installed Pegasus can take complete control of a device, including accessing messages from apps like WhatsApp, and turning on the camera

and microphone. However, the capabilities required to detect Pegasus are scarce (*How does*, 2021). Detecting spyware is also risky and often remains the prerogative of specialised security sector teams and companies since the necessary "hacking" is illegal in many jurisdictions and voids the warranty of the mobile device.

In the Pegasus scandal, the technical researchers from the international civil society groups AmnestyTech and CitizenLab developed a methodology to detect and document spyware infections on mobile devices (Amnesty International, 2021). Both groups have long been sounding the alarm over the abuse of spyware but only recently managed to attract wider attention in Europe. While some companies have the same technical capabilities as AmnestyTech and CitizenLab, corporate security analysts do not prioritise detecting and documenting spyware on the phones of journalists. Government-administered security agencies are clients of companies like NSO and have an interest in the tool remaining undetected and therefore do not put resources into detection capabilities.

Tracing and documenting illegal spying are essential steps for accountability. However, the scarcity of available forensic capabilities globally limits the scope of how many devices can be examined. It is thus safe to assume that we are only seeing the tip of the iceberg.

3 Ineffective oversight and limited accountability for Pegasus in Europe

Following the Pegasus revelations in June 2021, most European governments provided short-lived responses, while parliaments, oversight bodies and civil society were more decisive in uncovering and addressing the factors contributing to illegal spying in Europe.

One of the most vocal critics of the Pegasus revelations has been the European Data Protection Supervisor (EDPS) Wojciech Wiewiórowski. While the EDPS acknowledges that grave interference with human rights can be justified in the presence of serious threats to national security, they must be necessary, proportionate and prescribed by law (EDPS, 2022, p.7). EU member states undertake this balancing act in their national laws regulating 'wiretapping' or 'government hacking', by relying on judicial procedures and through oversight bodies, which helps to explain why security agencies in Spain (J. Jones, 2022), Poland (Poland, 2022), and Hungary (Top Hungarian, 2021), were quick to insist that they had always acted within the law.

However, the EDPS' assessment of Pegasus was damning: The "level of interference with the right to privacy is so severe that the individual is in fact deprived of it" and concluded that the "regular deployment of Pegasus or similar highly intrusive spyware technology would not be compatible with the EU legal order" (EDPS, 2022, p.8). The

EDPS ultimately aligned with civil society and called for a complete ban on the development and deployment of spyware with Pegasus-like capabilities in Europe (EDPS, 2022, p.9).

Whether the threats to national security are indeed grave enough to justify the use of Pegasus as necessary and proportionate cannot be independently evaluated since the required information tends to be highly classified or has not been shared by any of the security agencies in Europe. The case has made it amply clear that existing legal frameworks and oversight institutions both on a national and a European level (such as the EDPS) are inadequate for governing - and limiting - the purchase and deployment of a software such as Pegasus, and preventing the infringement on fundamental rights that it entails. Since national security is the responsibilities of member states, the EU has limited authority here. However, as the case evolves, the distribution of competencies will require a critical discussion also considering the state of rule of law in different EU countries.

So far, the European Commission has not opened an investigation referring to member state competencies on questions of national security (Nielsen, 2022). The European Parliament (EP) set up a dedicated committee on the 'Use of Pegasus and equivalent surveillance spyware (PEGA)' in March 2022 seeking to uncover the unlawful use of Pegasus and other spyware (European Parliament, 2022a). To date victims, researchers, journalists and representatives of Google, Apple, Meta and Microsoft have testified against the use of spyware (European Parliament, 2022b). NSO Group's General Counsel and Chief Compliance Officer also stressed that better standards for the industry would be welcome (European Parliament, 2022c). PEGA also undertakes specific country visits to meet local representatives.

3.1 Restrained responses by EU governments

National governments are responsible for national security questions in the EU and are thus the competent authorities to address the abuse of Pegasus spyware. To date, responses have been somewhat restrained and political will seems to correspond with the state of the rule of law in the respective countries, for example with governments in Hungary and Poland denying any wrongdoing.

In France, the use of Pegasus against journalists was attributed to Moroccan intelligence. A Paris prosecutor opened a probe in July 2021 following a complaint[1] that

[1] RSF lawyers drafted the complaint based on invasion of privacy (article 216-1 of the French penal code), violation of the secrecy of correspondence (article 226-15), fraudulent collection of personal data (article 226- 18), fraudulent data introduction and extraction and access to automated data systems (articles 323-1, 3, 462-2), and undue interference with the freedom of expression and breach of the confidentiality of sources (article 431-1).

two French Moroccan journalists filed with the support of Reporters Without Borders (RSF), calling for the identification of the responsible party (Reporters without Borders, 2021). The French government convened an exceptional defence council however all information from the council remains classified. Morocco denied all allegations and pursued to file a defamation lawsuit against Amnesty International and Forbidden Stories (*Project Pegasus,* 2021).

In Spain, where the Prime Minister and individuals of the Catalan independence movement were targeted, the government pledged to convene a parliamentary oversight commission with access to classified information and stated that the security services will conduct an internal investigation. The Spanish Ombudsman also stated that it would investigate the government's alleged abuse of Pegasus (J. Jones, 2022). Shortly thereafter, the Spanish government fired the chief of intelligence (S. Jones, 2022). CitizenLab also informed **the UK** that it detected Pegasus on government networks close to Boris Johnson's office, allegedly linked to UAE controlled servers (Deibert, 2022).

The **Polish government** admitted to the use of Pegasus following weeks of denial in January 2022. The Polish senate, currently held by the opposition with a small margin, opened an investigation into the surveillance of political groups critical of the government with the ruling party 'PiS' actively opposing the inquiry. PiS also blocked a wider-reaching parliamentary inquiry in the lower house (Gera, 2022). Following the hearings, lawmakers announced their intention to draft a law regulating spyware (Walker, 2022). However, chances for success are slim given the fact that the Polish government flat out refused to cooperate with the PEGA committee on its visit to Poland and declined an invite to meet (van Sant, 2022). In **Hungary**, the investigating prosecutor dropped the case entirely, concluding that no harm was caused, and no crime was committed. The data protection authority did not identify violations regarding the use of Pegasus either (*Hungarian*, 2022) - a stark contrast to the assessment of the EPDS.

Reportedly**, Germany's** federal criminal police also bought Pegasus to fight terrorism and organised crime despite legal advice clarifying that the tool is not in line with German privacy law (*German police*, 2021). Despite specific parliamentary requests and a new government critical of surveillance practices, the responsible Ministry of Interior refuses to provide information whether Pegasus was used by German security agencies or not, citing security sector priorities and a corresponding need for secrecy (Meister, 2022). Even less information is available about the alleged purchase and use of Pegasus by **Belgium's** federal police (Klingert, 2022) and the **Dutch** intelligence services (Stuart Leeson, 2022).

A related spyware scandal in **Greece** unfolded from April to August 2022 and only after the opposition leader was targeted with 'Predator', a spying tool similar to Pegasus. Earlier calls for accountability by affected journalists had only led the government to

change the law in order to keep sensitive information about spying under wraps (Tsimitakis, 2022). Intellexa, a company that markets predator spyware is registered in Greece and allegedly has links to the government (Telloglou & Triantafillou, 2022). Nevertheless, Prime Minister Mitsotakis denied any wrongdoing and initially attributed the spying to private individuals. However, under continued pressure the head of Greece's national intelligence service and the government's secretary general were eventually removed from their positions (Tsimitakis, 2022). A parliamentary inquiry set up to investigate the scandal actively blocked testimonies of those directly involved with Predator including the CEO of Intellexa. The EP's PEGA committee is scheduled to travel to Greece in November 2022 (Mandilara, 2022).

Greece's use of 'predator' spyware further exemplifies that policy responses to spyware use in Europe need to be systemic in nature and cannot be focused on a single tool, such as Pegasus.

3.2 The foreign policy dimension of spyware trade

NSO Group, alongside many other spyware vendors, is based outside the EU which makes it even more difficult to access information about its clients or regulate the company. The Israeli Ministry of Defence grants export licenses to NSO Group and civil society attempts to challenge the licenses in court have failed (Amnesty International, 2022). At the same time, European governments prioritise good relations with Israel over transparency of the industry and accountability for abuses carried out with Israeli-made spyware.

Similarly, it appears that there have been no consequences to the relations between Morocco and France or the UAE and the UK following allegations of spying on France's President Emmanuel Macron and the hacking of networks in Downing Street respectively. On the contrary, the Moroccan government filed a defamation lawsuit against Amnesty International and Forbidden Stories with the Paris criminal court (Pegasus Affair, 2022).

In January 2022, the Ministry of Foreign Affairs of Finland stated that following an internal investigation it had detected that Pegasus was used against its diplomats abroad (*Finnish Diplomats*, 2022), demonstrating the risk Pegasus-like spyware poses to diplomatic protocol and the integrity of diplomatic communication.

4 Lack of transparency and oversight in the global surveillance industry

A growing number of private spyware firms develop and sell sophisticated surveillance technologies to law enforcement agencies in the EU in response to the increased adoption of more secure end-to-end encrypted communications. The development,

trade and use of spyware is extremely untransparent and lacks meaningful regulation or public scrutiny (Pollet, 2022).

Due to the continuous pressure of global civil society coalitions, NSO Group has started to provide a few insights into the industry and its practices, while suggesting that other actors are likely to have even lower levels of transparency (NSO Group, 2021, p.8).

In its first 'Transparency and Responsibility' report published 30 June 2021, NSO reacted to some allegations, stressing Pegasus' crucial role in preventing and solving grave crimes and a strong commitment to human rights standards. It also reiterates that Pegasus is only licensed to vetted, legitimate state intelligence and law enforcement agencies via human rights due diligence procedures that are not operated by NSO. Misuse should lead to termination of the license (NSO Group, 2021, p.7-9). Responding to civil society concerns, one of NSO's investors Novalpina Capital echoed NSO's position. It also expressed full trust in NSO's procedures (Amnesty International, 2019).

Tellingly, however, both parties take no issue with the fact that Pegasus violates human rights by design, that conducting due diligence of EU clients is entirely at the discretion of the vendor and that there is a lack of mechanisms to independently assess NSO's practices and Pegasus' actual performance. Currently, it is impossible to assess whether established due diligence measures are adequate and whether Pegasus is a decisive factor in addressing serious crimes. During the European Parliament's PEGA committee hearings in June 2021, NSO clarified that at least 5 European countries still used Pegasus while one contract had been terminated (Roussi, 2022) –a larger number of EU states using Pegasus than initially confirmed. The hearing also showed that lawmakers still struggle to understand how NSO Group operates due to opaque corporate structures (Manancourt, 2022).

Only following the hearings and the EP's committee visit to Israel in July 2022, European parliamentarians and the public learned that overall, 14 EU member states bought Pegasus. At the time of writing, 12 of 14 states were using 15 Pegasus systems and two contracts had been terminated. Aside from the publicly known cases, it remains unclear which other European states are NSO's clients and whether the list of 14 is complete (Biselli, 2022).

Against the backdrop of documented abuses, misleading or incomplete information sharing by NSO and the limited sources to obtain reliable information, it is hardly surprising that civil society and some US-based companies remain united in their call against the spyware industry. Meta took NSO to court already in 2019 and continues further efforts to ban surveillance-for-hire actors from its platform (Agranovich, 2021). Apple, whose products were compromised by NSO, forbids unauthorised access in its Software License Agreement (Apple, 2022a, p.5). Apple filed a lawsuit against NSO in

the US and announced a 10 million dollar contribution to support advocates and researchers (Apple, 2021). Moreover, Apple presented industry-wide, unprecedented, technical countermeasures, rolling out a new "Lockdown Mode" for high-risk iPhone users. The lockdown mode drastically reduces the threat surface – put simply: the amount of code that can be attacked - by disabling a wide array of functions with potentially vulnerable software such as message attachments, wired connections and web browsing (Apple, 2022b).

While the US government has sanctioned NSO, we have yet to see industry wide measures and efforts to hold NSO to account in Europe (Lyngaas, 2021). Existing state and EU level laws pertaining to supply chains, due diligence and export control have not managed to bring greater transparency and accountability into the industry, leaving it to companies and civil society to use the mechanisms at their disposal, as for example legal action or public pressure. However, regulating the surveillance industry can only be effective if lawmakers and companies step up decisively and consider the wider ecosystem of technical enablers, including the buying and selling of zero-click exploits, in their regulatory efforts.

4.1 Zero-click exploits and responsible disclosure standards

Spyware, like Pegasus, that can be installed remotely without any action by the target often relies on zero-click exploits to gain access to the device. These vulnerabilities are usually found by hackers and security researchers in the source code of a device and get fixed once the vendors of the software become aware of them. Exploits are thus short lived and hard to come by. Law enforcement agencies and private surveillance companies have a vested interest in keeping them secret as long as possible since they actively buy vulnerabilities from hacking communities and exploit them to gain access to a suspect's device (*How does Pegasus,* 2021).

Companies like Google and Meta, whose products are being hacked, offer competitive bug bounty programs with the goal to incentivise hackers, security researchers and penetration testers to report vulnerabilities directly to them (Das, 2022). In the case of Pegasus, however, Apple was not aware of the iOS exploit and Google's security analysts later stated "...this to be one of the most technically sophisticated exploits we've ever seen..." (Beer & Groß, 2021). With the launch of the new "Lockdown Mode", Apple added a new category to its bug bounty program rewarding up to 2 million dollars to researchers that find vulnerabilities in "Lockdown mode" (Apple, 2022b). Creating incentives for researchers to focus on a reduced threat surface may well enable Apple to better secure the iPhones of high-risk users.

This is an area where governments have so far been punching under their weight. To date, government policies enabling the safe identification and disclosure of vulnerabilities have not caught up with industry standards and security needs, with only few European countries having disclosure policies implemented (ENISA, 2022). During the EP hearing, company representatives actively called on EU lawmakers to

create a legal environment that enables companies to address the issue (Pollet, 2022). Interests of civil society and technical experts tend to overlap, arguing that not regulating the identification and trade of zero-click exploits poses a severe risk to privacy and related rights and has the potential to harm critical public infrastructure.

The recently published draft proposal of the Cyber Resilience Act includes EU-wide requirements for vulnerability disclosure processes, which – if implemented without exceptions for law enforcement and clear legal security for researchers – will be an important step in the right direction (European Commission, 2022).

5 Inadequate remedies for victims

Another area that merits increased attention from the side of policy makers is the expansion of the possibilities for the victims of spyware to seek redress both from their government as well as from the producers of spyware itself. EU and member states do not have victim-centred mechanisms in place to assist or compensate victims in mitigating the negative impact of unlawful surveillance. Despite strong privacy provisions in European legislation, victims also have no way to find out what information was collected about them and for what purpose, who has access to the information and how it can be deleted. At the time of writing, legal proceedings to hold the responsible party to account for unlawful spying were underway in France. Reporters Without Borders also formally referred 17 victims to four UN special rapporteurs (Reporters without borders, 2021).

Civil society organisations like Amnesty International, Citizen Lab, Access Now, Amnesty International, Reporters without Borders and many others are pushing for systematic reforms and have assisted victims to navigate options to seek redress for the abuses, improve their digital security, receive phone examinations and legal remedy and access international mechanisms, for example at the UN level.

6 Conclusion

Since the publication of the Pegasus project in July 2021, targeted spyware has received lots of attention by media, civil society, companies, and parliaments. Yet, little has been done by governments and law enforcement agencies to address the underlying issues and bring about systemic change. Parliamentarians and oversight institutions like the EPDS alongside companies like Meta, Apple, Microsoft and Google are questioning security sector priorities, attributing the growing demand for commercial spyware to government agencies and seeking stronger regulations and oversight for both law enforcement and spyware developers. The absence of political will for an overarching reform effort demonstrates that governance of Pegasus and similar tools is still exclusively under the purview of security agencies and follows

"national security interests" as defined by security sector actors. A continued hands-off approach towards the trade of zero-click exploits and the private surveillance industry further illustrates that stance.

Civil society actors have taken on the function as public watchdog and had a decisive impact on identifying abuses, making their impact visible, mobilising public opinion and mounting pressure, specifically on NSO. Companies like Meta, Microsoft and Google, usually criticised by civil society, found their demands for stronger state regulations aligned with rights-protecting groups. Ongoing parliamentary inquiries and civil society investigations have constraint mandates and authority to address the security sector dimension, and rely, for example, on parliamentary hearings for information. The case shows clear limitations in activism to trigger systemic reform—even when aligned with big tech companies—vis-a-vis security sector norms and actors.

While EU governments cannot regulate surveillance companies outside of EU jurisdiction, political will can bring change to the trade and use of spyware within Europe. **For governments** these could include *effective* import/export control regimes for spyware overseen by an independent entity, strict rules defining government procurement of spyware that include transparency, oversight and limits on what can be purchased and from whom based on human rights considerations or outright bans for tools that are not in line with European fundamental rights by design. Governments can also create legal security for security researchers identifying breaching and vulnerabilities. To address the foreign policy dimension, governments could apply targeted sanctions for spyware companies with existing records of abuse as well as investors benefiting from the abuses.

Opportunities to step up **corporate responsibility** efforts can, for example, include restrictions on investments in spyware companies and proactive divestment of already invested capital. Developers can integrate safety features in the design that can be controlled by oversight institutions and platforms, and infrastructure providers can ban spyware from their platforms. Liability can be increased for technical enablers facilitating the supply chains of spyware. Finally, companies can set up robust and competitive vulnerability disclosure regimes designed to drastically reduce the availability of zero-click exploits on the black market.

However, in the absence of political will, the possibility for redress depends on legal action taken by affected parties, resulting in a protracted case-by-case approach to the issue. Successes of individual complaints are entirely reliant on the independence of courts (as seen in Hungary), require considerable resources, robust evidence and long-term commitment. Abuses can continue until a final court decision is reached that goes beyond individual compensation of victims and requires law makers to act. Hence, individualised accountability approaches can also work as a stalling tactic, benefiting those in favour of the status quo. Whether ongoing litigation efforts will be

successful or will contribute to systemic change in the governance of spyware in Europe remains to be seen. Companies and civil society should continue to pressure governments and further focus on assessing the impact of spyware on public trust in institutions and the integrity of democratic processes, as well as mental health effects on affected communities. Most importantly, advocates should continue to make the impact of spyware more tangible and less abstract in order to harness democracy's most important accountability mechanism: voters.

7 Bibliography

Agranovich, D. (2021, December 16). *Taking Action Against the Surveillance-For-Hire Industry*. Meta. https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire

Amnesty International. (2019, April 19). *Novalpina Capital's response to NGO coalition's open letter (18 February 2019)*. https://www.amnesty.org/en/documents/doc10/0210/2019/en/.

Amnesty International. (2021. July 18*). Forensic Methodology Report: How to catch NSO Group's Pegasus*. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/.

Amnesty International. (2022, July 12). *Israel: Court rejects bid to revoke notorious spyware firm NSO Group's export license*. https://www.amnesty.org/en/latest/news/2020/07/israel-court-notorious-spyware-firm-nso/.

Apple. (2022a, June 25). *iOS and iPad OS Software License Agreement*. https://www.apple.com/legal/sla/docs/iOS15_iPadOS15.pdf.

Apple. (2022b, July 6). *Apple expands industry-leading commitment to protect users from highly targeted mercenary spyware*. [Press release]. https://www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware/.

Apple. (2021, November 23). *Apple sues NSO Group to curb the abuse of state-sponsored spyware: Apple also announced a $10 million contribution to support cybersurveillance researchers and advocates*. [Press release]. https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

Bajak, F., & Gera, V. (2021, December 21). AP Exclusive: Polish opposition duo hacked with NSO spyware. *AP NEWS*. https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e

Beer, I., & Groß, S. (2021, December 15). A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution. Google Project Zero. https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html

Bleyer-Simon, K. (2021, August). Pegasus in Hungary: A Surveillance State Unmasked. *Heinrich Boell Stiftung*.https://eu.boell.org/en/2021/08/24/pegasus-hungary-surveillance-state-unmasked

Business and Human Right Resource Centre. (2021, September 27). *Investigation finds NSO Group spyware sold to governments used against activists, politicians & journalists; company denies allegations: Timeline*. https://www.business-humanrights.org/en/latest-news/nso-group-spyware-sold-to-governments-used-to-target-activists-politicians-journalists-according-to-pegasus-project-investigation-company-denies-allegations/

Das, A. (2022, February 17). Bug Bounty Programs by the World's Biggest Tech Companies. *Geekflare*. https://geekflare.com/tech-companies-bug-bounty-programs/

Deibert, R. (2022, April 18). UK Government Officials Infected with Pegasus. *Citizen Lab*. https://citizenlab.ca/2022/04/uk-government-officials-targeted-pegasus/

European Commission. (2022, September 15). *New EU New EU cybersecurity rules ensure more secure hardware and software products*. [Press release]. https://digital-strategy.ec.europa.eu/en/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products

European Data Protection Supervisor. (2022, February 15). Preliminary Remarks on modern spyware. https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf

The European Union Agency for Cybersecurity. (2022, April 13). *Coordinated Vulnerability Disclosure policies in the EU*. [Press release]. https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu

European Parliament. (2022a, June 25). Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware. https://www.europarl.europa.eu/committees/en/pega/home/highlights

European Parliament. (2022b, June 19). *Pegasus inquiry: MEPs and experts discuss security, supervision, and the role of Big Tech*. [Press release]. https://www.europarl.europa.eu/news/en/press-room/20220610IPR32722/pegasus-inquiry-meps-and-experts-discuss-supervision-and-the-role-of-big-tech

European Parliament. (2022c, June 20). *Pegasus: MEPs grilled NSO Group representatives about spyware abuse allegations*. [Press release]. https://www.europarl.europa.eu/news/en/press-room/20220620IPR33414/pegasus-meps-grilled-nso-group-representatives-about-spyware-abuse-allegations.

Finnish diplomats targeted with Pegasus spyware-ministry. (2022, January 28). *Reuters*. https://www.reuters.com/article/us-finland-security-spyware-idUSKBN2K217l

Gera, V. (2022, January 17). Polish senators question cyber experts in hacking inquiry: A Polish Senate commission has opened an investigation into the use of powerful spyware against government critics. *Abc News*. https://abcnews.go.com/International/wireStory/polish-senators-question-cyber-experts-hacking-inquiry-82310425

German police secretly bought NSO Pegasus spyware: Sources have confirmed media reports that federal criminal police purchased and used the controversial Israeli surveillance spyware despite lawyers' objections. (2021, September 7). *Deutsche Welle*. https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197

Gijs, C. (2022, May 2). Spanish PM Pedro Sánchez had phone hacked with Pegasus spyware. *Politico*. https://www.politico.eu/article/pegasus-spyware-targeted-spanish-pm-pedro-sanchez-defense-minister/

How does Pegasus Work? (2021, July 18). *OCCRP*. https://www.occrp.org/en/the-pegasus-project/how-does-pegasus-work

Hungarian prosecutors drop probe into Pegasus spyware. (2022, June 15). *Daily News Hungary*. https://dailynewshungary.com/hungarian-prosecutors-drops-probe-into-pegasus-spyware/

Jones, J. (2022, April 24). Spain's ombudsman to probe alleged cyber spying of Catalan figures. *Reuters*. https://www.reuters.com/article/us-spain-politics-catalonia-spying-idCAKCN2MG0A6

Jones, S. (2022, May 10). What we know about Spain's cyber-espionage spyware scandals: Spain's Pegasus spyware revelations have come to a head with the sacking of the country's spy chief. *The Guardian*. https://www.theguardian.com/news/2022/may/10/what-we-know-about-spains-cyber-espionage-spyware-scandals

Klingert, L. (2022, April 21). Belgian police reveal use of controversial Pegasus spyware. *The Brussels Times.* https://www.brusselstimes.com/belgium/218350/belgian-police-use-controversial-pegasus-spyware

Lyngaas, S. (2021, November 8). US blacklists Israeli firm NSO Group for use of spyware. *CNN*. https://edition.cnn.com/2021/11/03/tech/nso-group-us-blacklist/index.html

Manancourt, V. (2022, May 20). Pegasus' complex structure hinders EU spyware probe: Byzantine corporate structure is hampering lawmakers' action to stop spyware in Europe. *Politico.* https://www.politico.eu/article/europe-pegasus-spyware-eu-probe-nso/

Mandilara, S. (2022, October 4). EP PEGA Committee to investigate Greek spyware scandal on the ground. *Euroactiv*. https://www.euractiv.com/section/politics/short_news/ep-pega-committee-to-investigate-greek-spyware-scandal-on-the-ground/

Matriche, J. (2021, July 28). « Projet Pegasus »: le téléphone de Charles Michel sélectionné quand il était premier ministre de la Belgique. *Le Monde*, https://www.lemonde.fr/pixels/article/2021/07/20/projet-pegasus-le-telephone-de-charles-michel-selectionne-quand-il-etait-premier-ministre-de-la-belgique_6088962_4408996.html

Meister, A. (2022, June 24). Bundesregierung verweigert Antwort zu NSO Pegasus. *Netzpolitik*. https://netzpolitik.org/2022/staatstrojaner-bundesregierung-verweigert-antwort-zu-nso-pegasus/

Nielsen, N. (2022, April 17). EU Commission won't probe 'Pegasus' spyware abuse," *Euobserver*. https://euobserver.com/digital/154752

NSO Group. (2021, June 30). *Transparency and Responsibility Report 2021*. https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf

Pegasus Affair: Morocco sues Amnesty International, French NGO for defamation. (2022, July 22). *France24*. https://www.france24.com/en/africa/20210722-morocco-files-libel-suit-in-france-against-ngos-alleging-it-used-pegasus-spyware

«Projet Pegasus»: le Maroc attaque Forbidden Stories et Amnesty International en diffamation. (2021, July 23). *Le Monde with AFP and Reuters.* https://www.lemonde.fr/projet-pegasus/article/2021/07/22/projet-pegasus-emmanuel-macron-convoque-un-conseil-de-defense-exceptionnel_6089148_6088648.html

Poland: Kaczyński has no problem with the use of Pegasus. (2022, January 10). *Visegrad Post*. https://visegradpost.com/en/2022/01/10/poland-kaczynski-has-no-problem-with-the-use-of-pegasus/

Pollet, M. (2022, June 16). Big Tech points finger to governments for driving surveillance technology demand. *Euroactive*. https://www.euractiv.com/section/cybersecurity/news/big-tech-points-finger-to-governments-for-driving-surveillance-technology-demand/

Reporters without Borders. (2021, July 20). *After Pegasus revelations, RSF and two Moroccan-French journalists file complaint in Paris*. [Press release]. https://rsf.org/en/after-pegasus-revelations-rsf-and-two-moroccan-french-journalists-file-complaint-paris

Reporters without Borders. (2021, August 6). *NSO/Pegasus: 17 journalists from 7 countries join RSF's complaint in Paris and before the UN*. [Press release]. https://rsf.org/en/nsopegasus-17-journalists-7-countries-join-rsfs-complaint-paris-and-un

Roussi, A. (2022, June 21). Pegasus used by at least 5 EU countries, NSO Group tells lawmakers: NSO Group 'made mistakes,' its chief lawyer says. *Politico.* https://www.politico.eu/article/pegasus-use-5-eu-countries-nso-group-admit/

Satter, R., & Bing, C. (2022, April 11). Exclusive: Senior EU officials were targeted with Israeli spyware. *Reuters.* https://www.reuters.com/technology/exclusive-senior-eu-officials-were-targeted-with-israeli-spyware-sources-2022-04-11/

Scott-Railton, J., Elies Campo, E., & Marczak, B. (2022, April 18). CatalanGate: Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru. *Citizen Lab*. https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

Stuart Leeson, S. (2022, June 3). Dutch intelligence service allegedly uses Pegasus hacking software. *Euroactiv*. https://www.euractiv.com/section/politics/short_news/dutch-intelligence-service-allegedly-uses-pegasus-hacking-software/

Telloglou T., Triantafillou, E. (2022, May 25). The line that connects the Greek government with Intellexa. *Inside Story*. https://insidestory.gr/article/i-grammi-poy-syndeei-elliniko-dimosio-me-tin-intellexa

Top Hungarian Official Admits Government Bought Pegasus Spyware. (2021, November 4). *RFERL Hungarian Service*. https://www.rferl.org/a/hungary-admits-pegasus-spyware/31546293.html

Tsimitakis, M. (2022, September 21). Greek PM's Wiretapping Scandal Can't be Justified by Foreign Threats. *Balkan Insight*. https://balkaninsight.com/2022/09/21/greek-pms-wiretapping-scandal-cant-be-justified-by-foreign-threats/

Van Sant, S. (2022, September 21). Poland 'hiding' from spyware inquiry, EU lawmakers warn. *Politico.* https://www.politico.eu/article/poland-hiding-from-spyware-inquiry-eu-lawmakers-warn/

Walker, S. (2022, January 24). Polish senators draft law to regulate spyware after anti-Pegasus testimony: Senate commission plans reform after hearing how NSO software used against government critics. *The Guardian.* https://www.theguardian.com/world/2022/jan/24/polish-senators-draft-law-to-regulate-spyware-after-anti-pegasus-testimony

Hertie School
Centre for
Digital Governance

Friedrichstraße 194
D – 10117 Berlin
Tel.: +49 (0)30 259219-0

Online: hertie-school.org/centre-for-digital-governance/
E-Mail: info@hertie-school.org
Twitter: @thehertieschool