LmunA 2022

Research report

Forum:	European Parliament
Issue:	Investigating the usage of Pegasus and similar surveillance spyware
Student Officer:	Julian van Halteren
Position:	Main Chair

LMUNA
Lorentz Lyceum
Model United Nations
Arnhem

Table of Contents

Introduction

The theme of this year's LmunA conference is emerging technologies in shaping modern society. While incorporating more and more advanced technologies into more and more aspects of our daily lives has certainly made our lives easier, it comes with a dark side that is still too often underexposed. Technologies, especially those connected to the Internet, will always carry the risk of being hackable. And the more and more the use of technology emerges in our society, the more important it becomes to be aware of this vulnerability and to do something about it.

In 2019, it was revealed that software called Pegasus had been used to spy on at least 50,000 phones without the targets knowing. This software, created by an Israeli commercial company called NSO Group, uses so-called zero-day exploits which are vulnerabilities that are not yet known by the company behind the software that can be used to bypass the security of a device to install malicious software on it. The Pegasus software used various ways to get installed on a device although most of them were techniques that didn't require the target to click on something themselves to be installed. The software could be installed by calling a target's number or sending them a message via iMessage. Although NSO Group does not disclose to whom it sells its software, which is supposedly designed to track terrorists and criminals, leaked documents showed that authoritarian regimes such as Saudi Arabia use the software to spy on human rights activists and journalists. Hungary and Spain have also been shown to use the software for this purpose. The NSO Group is one of many companies selling this kind of software and if one company stinks like this, we can only imagine the state of the whole industry.

We first got a wake-up call back in 2013 when Edward Snowden leaked documents to The Guardian revealing the National Security Agency's (NSA) mass surveillance of the world's online population. In the years that followed, we saw countries exerting increasing control over their intelligence services to limit these practices, and with success. However, this sector is developing at a furious pace and new challenges are constantly coming our way.

However, we must also realize that surveillance programs are a vital part of the work of intelligence services, a part that will only become more important with the growing cyber and terrorist threats. The intelligence obtained from surviving surveillance programs has helped catch countless criminals and prevent several terrorist attacks.

Now that we see spyware being used to spy on the lives of journalists and human rights activists even in European democracies, it is time for a genuine discussion on its use. Does the benefit of tracking down terrorists and criminals compare to the abuse that can be made from this software? And where do we stop hacking and spying? Now 50,000 phones were spied on, but as we have seen in the past, governments are only too eager to scale this up to the millions. This is a discussion that reveals some fundamental questions of our time: To what extent do we allow governments to restrict our privacy in order to promote our security and to what extent do these surveillance programs infringe on fundamental human rights? In a world where hacking tools are the fastest growing market and are sold alongside guns and tanks by increasingly powerful companies, it is time for regulation. For conventional weapons and their vendors, there are strict rules, but these do not exist for spyware yet in cyberspace. It is now up to us, the European

Parliament, pioneers in the field of digital legislation, to set an example and shine a light in this dark sector.

Since this is an MEP-style debate, it is important to realize that one must follow the viewpoint of his or her given party. Individual countries matter little, as we are trying to solve problems at the European level.

In this research report, the focus will be on spyware used by governments, just like Pegasus.

Definitions of key terms

Spyware

Spyware is malicious software that enters a user's computer, gathers data from the device and user, and sends it to third parties without their consent.

Cyber Surveillance Tools (CSTs)

Software used to digitally track users on the internet.

Zero-day exploit

A zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability—hence "zero-day."

The Wassenaar Arrangement

The Wassenaar Arrangement is an export control regime with 41 participating states that promotes transparency of national export control regimes on conventional arms and dual-use goods and technologies.

Dual-use goods

Dual-use items are goods, software, and technology that can be used for both civilian and military applications.

Zero-day exploit

A zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability—hence "zero-day."

General overview

Spyware is a type of malicious software (malware) that gathers data from your computer without your consent. Without the target realizing it, the spyware can read messages and emails, record keystrokes, switch on the camera and microphone, and so on. Software that collects data but requires the user to sign an End-User License Agreement (EULA) is not spyware. Although there are many different types of spyware, the aim is always to be installed without being

detected, to hack into the network, and in most cases to remove itself safely. Spyware is mainly used by criminals to steal data, but governments also create and use the software, which is often referred to as policeware. Spyware often includes adware, which is software that is downloaded and collects information about the user in order to use it for advertising purposes. The line between the two is very blurred.

The use of spyware by governments remains a vague, often unregulated area in many countries, including the EU. Governments have developed many types of spyware in the past, as became clear after the leak of the Vault 7 documents by Wikileaks, which showed that the American CIA had highly advanced hacking tools at its disposal, including spyware. Today, intelligence services in the USA must have a judicial warrant to install spyware, and in the UK, Germany, Austria, and Italy, among others, there are already laws at the national level restricting the use of spyware by governments.

The term "Spyware" originates from a Usenet post from 1995 in which Microsoft's business model is ridiculed as being hardware used for spying. Later, after toy manufacturer Mattel developed educational software that sent information back to Mattel itself, the term was popularized after a report by cybersecurity firm ZoneAlarm.

Spyware is used by governments as part of their digital surveillance programs, which emerged in the western world mainly after 9/11. In the aftermath, the power of software for governments worldwide has become clear. An increasing number of companies selling commercial hacking tools took advantage of this. Although the first such surveillance companies were established as early as the 1990s, they began to grow rapidly after 9/11. These companies design software, such as spyware and other hacking tools, and then sell them to governments. If it is up to the surveillance companies themselves at least, they can then use these tools to catch criminals and terrorists. Although these companies, for good reasons, always try to stay under the radar as much as possible and don't want to reveal their customers, there have been several leaks over the years, revealing that the companies sell their software not only to 'trustworthy' governments but also to countries known for violating human rights. It also became clear, especially after the Pegasus documents were released in the summer of last year, that these countries also target and eavesdrop on journalists, human rights activists, and other people working for the cause.

Spyware markets

At military markets such as Milipol and ISS World (i.e., the Wiretapper’s Ball), the stands of surveillance companies are increasingly present. Although 9/11 caused the first boom, the Arab Spring has set the second boom in motion. After this succession of revolutions, countries have become afraid that their regime could be next and surveillance software is obviously a useful tool in controlling the people. Although in the beginning many of these companies developed their products primarily for their own governments, they have increasingly started to market internationally. Today, about 75% of the companies sell their products internationally. Many of these companies, mainly from Western countries, not including China, have been proven to

market and sell their products to NATO and EU adversaries such as Russia. The emails from surveillance company The Hacking Team leaked by WikiLeaks in 2015 also made it painfully clear that these companies do not have their own moral compass. In these email exchanges between the company and governments such as those of Uzbekistan and Saudi Arabia, no questions about the use of the products were asked by these regimes.

It is a fact that developing cyber capabilities is becoming an increasingly privatized market. Why would a government invest a lot of money in developing these capabilities when they are available on the market? The result is that nowadays any state that has the money can buy cyber capabilities, whereas previously it was only a limited number of countries that had the right resources. While these tools can be useful for law enforcement, we see that through these markets they also end up in the hands of authoritarian regimes. A notorious example are the cyber capabilities developed by the UAE-based company DarkMatter, which were developed with the help of former US intelligence service employees and used to eavesdrop on US citizens. These companies pose a major proliferation risk while they still have free rein. The UN Special Rapporteur: “It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists…”

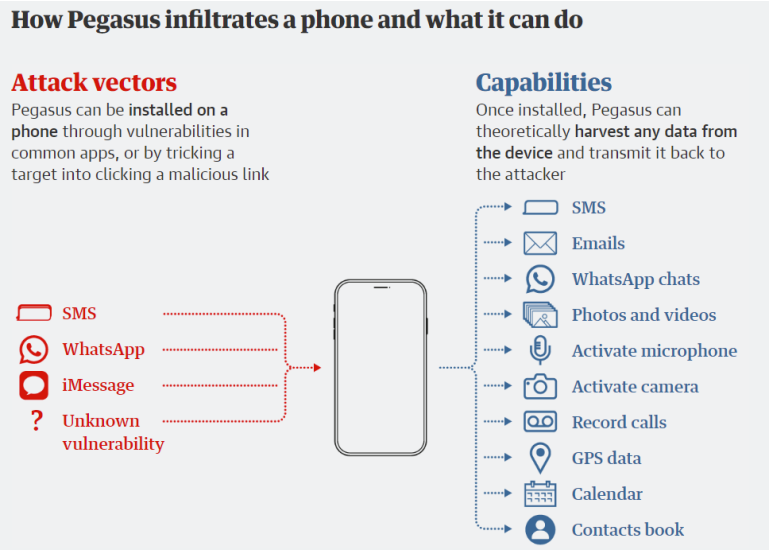
According to researchers from The Atlantic Council, it is mainly companies with interception or intrusion capabilities, which include spyware, that pose the greatest risk, partly due to the fact that these capabilities can be easily abused. The mere knowledge that an authoritarian regime has access to this kind of highly aggressive, offensive software and can use it to eavesdrop on you is enough to create a culture of fear and paranoia among anyone who has anything against this regime, and has already led to self-censorship.

Another important aspect of these markets is that it is often difficult to separate the authorities from these companies. According to various leaks and investigations by Netzpolitik, among others, the companies have ties to EU officials and lobbyists who have ensured, among other things, that despite a majority vote in the European Parliament, it was decided to significantly curtail the inclusion of human rights safeguards in the new regulations. Furthermore, it has also been shown that many employees switch between positions at surveillance companies and intelligence services where conflicts of interest can occur and, as has been shown in the past, information is taken to private actors.

The problem is not only that many of the companies sell their products to governments that are known not to be the most trustworthy, but also the fact that this is trade-in products that often exploit leaks in existing software, of which the creators themselves are unaware. This ensures that these leaks, also out of interest of the surveillance companies and their customers themselves, are not closed so that these leaks can potentially be exploited by anyone. However, it is also necessary to emphasize that there is not necessarily anything wrong with the market per se because the free market works in such a way that if there is demand for a legal product and there

are parties who can supply it, both parties can be satisfied. What goes wrong is the lack of regulation.

Pegasus Spyware



In the summer of 2021, it became painfully clear that the software of commercial companies is used for eavesdropping on citizens by authoritarian and non-authoritarian governments worldwide when the spyware Pegasus of the Israelian manufacturer NSO Group was found in the phones of more than 50,000 people worldwide after a massive leak. The leaked information was a list of telephone numbers of civilians designated by NSO Group's customers as persons of interest. Although not everyone on the list was actually infected with Pegasus, most were. The list included hundreds of business executives, religious figures, academics, NGO employees, union officials, and government officials, including cabinet ministers, presidents, and prime ministers. Of the telephone numbers selected, 1,000 were European citizens. Although NSO Group's clients probably also used the software to eavesdrop on criminals and terrorists, the vast majority of the telephone numbers in the dataset have no known connection to criminality.

NSO Group sells only to government agencies in over 40 countries and claims to do very extensive background checks to prevent human rights abuses. The Israelian government controls and determines to which governments NSO Group may sell. In this way, the Israeli government used NSO Group as a kind of component of the state, issuing licenses to countries with which the government would like to have a stronger diplomatic link. For example, applications from the government of Ukraine were also blocked by the government because of the fear of Russian anger. The company continues to emphasize that it has no knowledge of the customers' activities. They only supply the software.

NSO Group's signature software, Pegasus, works in such a way that it can penetrate an iOS or Android operating system and gain root access. This means that the software has complete and unrestricted access to all information, including videos, photos, and messaging, without the target realizing it, but can also switch on the camera and microphone, for example. Pegasus distinguishes itself further because the software can be installed on a device with a so-called "zero-click attack". In general, spyware is downloaded when the target clicks on a certain malicious link or opens a file. Action on the part of the target precedes this. Pegasus

distinguished itself because the target did not have to click on anything. The software can be installed by simply calling or sending an SMS to the target, for example. The software makes use of so-called "Zero-day exploits". These are exploits that the manufacturer is not yet aware of. Once Pegasus was installed, it managed to jailbreak the phone. This means that the restrictions imposed by the manufacturer can be circumvented. In most cases, it is virtually impossible to find out whether Pegasus was or is installed, partly because later versions of the software are only stored on the device's temporary memory instead of the hard drive, which means that any trace of the software is lost when the phone is switched off. What is very worrying about Pegasus is that it uses these "zero-day exploits" because that way even the most paranoid, security-conscious person cannot protect themselves from the software.

Pegasus was first found in 2016 when Arab human rights activist Achmed Mansoor reported a cyber-attack by text message. When researchers at Citizen Lab of the University of Toronto later investigated the software, they found it to be a highly sophisticated form of spyware. For two years, researchers investigated the software and found it on more than 1,500 phones and found that operations with the software were carried out in more than 45 countries. NSO Group eventually claimed to have sold Pegasus to 60 government agencies in 40 countries. In July 2021, several media outlets around the world, working together on the so-called Pegasus Project, came out with the story about the software at the same time.

Following the news, Apple has launched a lawsuit against NSO Group for using a "zero-day exploit" in iOS. Several governments, including the US, have blacklisted NSO Group. In July 2022, news emerged that US contractor giant L3 Harris wants to acquire the company, which had been in dire straits since the leak.

Pegasus in the EU

Several governments in the EU have admitted to buying Pegasus from NSO Group. According to research carried out by the PEGA committee of inquiry appointed by the European Parliament, at least five governments in the EU have actively used Pegasus. However, an NSO Group employee has leaked to the New Yorker that the tool has been sold to virtually every EU member state. The use of commercial spyware is officially condemned by the European Parliament. Earlier journalistic investigations showed that various EU countries were using Pegasus. These will be further discussed in the Major Parties Involved section.

Many leaders of EU Member States, such as France's President Emmanuel Macron and Spain's Prime Minister Pedro Sánchez, have been bugged with Pegasus, almost always it is unclear by which party. The list of those who have been spied upon also includes some members of the European Parliament (MEPs).

The structure of NSO Group appears from the ongoing investigation by the PEGA Committee to be much more complex than initially thought. Licenses have been obtained via many subsidiaries

that are difficult to trace. It recently emerged that Member States Bulgaria and Cyprus, although they both deny it, have granted export licenses to NSO Group.

Major parties involved

Hungary

Research by Hungarian news website Direkt36 shows that more than 300 Hungarian citizens, mainly lawyers, and journalists, were potentially tapped by the Hungarian government with Pegasus. It was notable that the leaders of the Presidential Guard of the Republic of Hungary and their families were tapped with Pegasus in 2019 and Victor Orbán's chief advisor Cecília Szilas, before her appointment, was also targeted. Although Hungary first denied using the software, the Minister of Justice later admitted to having used the software for law enforcement purposes. Hungary is the country in Europe that, according to the information now known, has used Pegasus the most

Poland

In Poland, Pegasus was probably used primarily to eavesdrop on high-ranking and former high-ranking officials of the ruling PiS party. In addition, journalists, lawyers, and people associated with the opposition party Civic were also bugged. Poland, after denying initial endorsements like Hungary, later admitted to using the Pegasus in accordance with the law.

Spain

In April 2022, researchers from Citizenlab released a report, called CatalanGate, about spyware, Pegasus, and the also Israeli Candiru, used by the Spanish government to spy on Catalan parliamentarians and activists. In some cases, the family members of these as well. 63 were targeted with Pegasus and four with Candiru. According to the Spanish newspaper El Pais, the Spanish intelligence service bought the National Intelligence Centre (CNI) Pegasus around the beginning of 2010. The Spanish government has admitted to having used the spyware, in accordance with the law but did start an investigation.

Between April and May 2021, Prime Minister Pedro Sanchez and Defense Minister Margarita Robles were also targeted by what they called an “illegal and external … attack” by an alien, foreign state agency.

France

In the EU, France was the country where most politicians were spied on. These include five to fourteen French cabinet ministers and President Emmanuel Macron, probably by known NSO client Morocco. In addition, some 7 activists and journalists have been infected, some of them in favor of an independent Western Sahara.

Israel

Israel, the country where the NSO Group is based, is of course an important party. It has become clear that the Israeli government used the powerful spyware in a diplomatic chess game. Israel's defense ministry had to approve every sale of the spyware and therefore has a major role in choosing which countries and which countries do not get the spyware. Although the Israeli government says it does everything according to the guidelines of the Wassenaar Arrangement, an international agreement to ensure that evil parties cannot get their hands on certain weapons, the leak contradicts this. The Israeli government also indicates that human rights were taken into account in the decision, although several anonymous Israeli officials contradict this. In fact, research by the New York Times found that several countries, including Mexico and Panama, were voting for motions by Israel in the UN General Assembly around the time they bought Pegasus from Israel, although this may have had to do with other factors as well. Furthermore, almost every country that signed the 2020 Abraham Accords, on normalizing ties with Israel, got the spyware. Israel, according to the Washington Post, has also used the spyware itself to spy on activists and opponents of President Netanyahu.

Timeline of Key Events

16 May 1996	Enforcement of the Wassenaar Arrangement
11 September 2001	Terrorist attacks in the US after which the US will invest much more in cyber-surveillance tools, causing private companies to grow
2010	First versions of Pegasus emerge
December 2010 – December 2012	Arab Spring causes Arabian regimes to buy surveillance tools
5 June 2013	Edward Snowden releases NSA documents revealing huge surveillance operations
In August 2016	Arab human rights activist Achmed Mansoor reports the first version of Pegasus to CitizenLab
25 May 2018	EU enforces General Data Protection Regulation (GDPR)

2 October 2018	Jamal Khashoggi is murdered in the Saudi-Arabian embassy in Ankara, Turkey. Later Pegasus is found on the phones of relatives
October 2019	Facebook sues NSO Group for using vulnerabilities in WhatsApp
July 2021	A journalist collaboration under the name of the Pegasus Project releases documents revealing a list of 50,000 people that have been spied on with Pegasus
3 November 2021	US blacklists NSO Group for participating in activities that undermine the national security
23 November 2021	Apple files lawsuit against NSO Group for targeting iOS users
March 2022	Establishment of the PEGA Committee
May 2022	Catalangate: researchers at CitizenLab reveal that the Spanish government used Pegasus and other spyware to spy on Catalonian politicians and activists
July 2022	US contractor L3 Harris is going to buy NSO Group in all likelihood

Previous attempts to solve the issue

The EU passed a law on the sale and export of surveillance software in October 2020. The law requires companies to obtain licenses from governments to sell products with military applications, to conduct research into the risks associated with human rights violations, and for governments to make these licenses public. Yet companies, like NSO Group, find ways around it with shady subsidiary companies. Further, the technology covered by these regulations is also still quite vague. Facial recognition, for example, is a technology that can be used for military purposes but is excluded.

Furthermore, in March 2022, the European Parliament voted to set up the PEGA investigation committee to investigate the use of Pegasus spyware by EU member states. They are to investigate existing laws and whether fundamental human rights have been violated and to what extent the software has been used for political purposes.

Additionally, in the EU, the 1995 Wassenaar Arrangement is in force. This is an agreement on the export of conventional and, since 2021 (Recast), also cyber-surveillance tools. The agreement is intended to regulate so-called Dual-Use items. These are technologies that can be used for both military and civilian purposes. The regulation stems from the idea that these technologies may not be freely exported if there is a risk that they will cause insecurity. Thus, since 2013, the

arrangement also explicitly targets so-called "Cyber Surveillance Tools" whose definition is given as being "dual-use items specially designed to enable covert surveillance of natural persons by monitoring, extracting, collecting, or analyzing data from information and telecommunication systems." The exporter has a duty to notify the authorities when he wants to export dual-use items that can potentially be used for destabilizing purposes. He also has a due-diligence obligation. When a member state wants to issue an export license for an item, it has to provide relevant information to the other member states and the Commission. Only if these agree can the license be issued. The Wassenaar Arrangement is non-binding and is virtually not enforced.

Possible solutions

As Edward Snowden pointed out in an interview with The Guardian in 2021, the market in cyber-surveillance tools is one that really shouldn't exist. The quickest solution would be an immediate ban on the commercial sale of this software. Since this step is still a long way off, it is first important to design a clear legal framework that includes human rights safeguards. Importantly, this new legal framework should be binding and well-enforced, unlike the Wassenaar Arrangement.

The UN Guiding Principles on Business and Human Rights is a useful guideline for setting up a framework in which businesses can be held accountable for their due diligence on human rights before selling their product. Another alternative to a framework would be a mutually agreed upon binding code like private security contractors have done after a whole series of scandals. This may work out better for these companies than harsh government regulations.

It is also important to look again at existing legal frameworks and treaties such as the European Convention on Human Rights and the European Court of Human Rights in which the privacy of EU citizens is also protected. Furthermore, there is also the EU Charter of Fundamental Rights and certain EU law directives such as the ePrivacy Directive that cyber-surveillance must comply with. The European Data Protection Supervisor (EDPS) has investigated in a report whether the use of Pegasus would be allowed according to these regulations. This is not the case, if only because it goes against the right to a fair trial. According to the EDPS, the EU should even move to a total ban on spyware with the same capabilities that Pegasus has. When this kind of software is used under exceptional circumstances, it should be under strict supervision, with a tight legal framework, and never for political reasons. The EDPS also recommends that the existing EU dual-use regulation be made stricter and broader.

There are also frameworks such as the Community Control Over Police Surveillance (CCOPS). Through this model, the police can directly request permission to purchase and use a cyber sovereign tool, then have to request feedback from the people before the tool can be used. In this way a total ban on certain technologies can be prevented. This framework already exists in several cities in the US including Seattle, where it has been successful so far.

Another way to stop international trade in surveillance software is to regulate exports. If the countries where the companies are located keep a strict eye on them, although there must be clear international agreements about this, the spread of the software can be stopped quite significantly. This, of course, must take into account networks to complicated subsidiaries as happened with NSO Group.

Further reading

IViR (Institute for Information Law). (z.d.). The new rules for export control of cyber-surveillance items in the EU. https://open.overheid.nl/repository/ronl-f616bafb-c268-436c-b926-3bacd98da61b/1/pdf/the-new-rules-for-export-control-of-cyber-surveillance-items-in-the-eu.pdf

Policy Department for Citizens' Rights and Constitutional Affairs. (z.d.). Pegasus and surveillance spyware. https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf

Robinson, K. (2022, 8 maart). How Israel's Pegasus Spyware Stoked the Surveillance Debate. Council on Foreign Relations. Geraadpleegd op 11 juli 2022, van https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate

Bibliography

The changes in the law that PEGASUS is forcing on the EU. (2022, 25 mei). StudenThinkTank. Geraadpleegd op 11 juli 2022, van https://esthinktank.com/2022/05/25/the-changes-in-the-law-that-pegasus-is-forcing-on-the-eu/

E. (2022, 7 juli). *Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets*. Atlantic Council. Geraadpleegd op 11 juli 2022, van https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/

Farrow, R. (2022, 18 april). *How Democracies Spy on Their Citizens*. The New Yorker. Geraadpleegd op 11 juli 2022, van https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens

Feldstein, S. (2021, 21 juli). *Governments Are Using Spyware on Citizens. Can They Be Stopped?* Carnegie Endowment for International Peace. Geraadpleegd op 11 juli 2022, van https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019/

G., G., Rebiger, S., G., & G. (2018, 29 oktober). *Surveillance exports: How EU Member States are compromising new human rights standards*. netzpolitik.org. Geraadpleegd op 11 juli 2022, van https://netzpolitik.org/2018/surveillance-exports-how-eu-member-states-are-compromising-new-human-rights-standards/#spendenleiste.

Jones, S. (2022, 16 mei). *Use of Pegasus spyware on Spain's politicians causing 'crisis of democracy'*. The Guardian. Geraadpleegd op 11 juli 2022, van https://www.theguardian.com/world/2022/may/15/use-of-pegasus-spyware-on-spains-politicians-causing-crisis-of-democracy

Kirchgaessner, S. (2021, 25 juli). *How NSO became the company whose software can spy on the world*. The Guardian. Geraadpleegd op 11 juli 2022, van https://www.theguardian.com/news/2021/jul/23/how-nso-became-the-company-whose-software-can-spy-on-the-world

Lloyd, J. (2022, 20 januari). *Protecting Society From Surveillance Spyware*. Issues in Science and Technology. Geraadpleegd op 11 juli 2022, van https://issues.org/surveillance-spyware-uso-group-pegasus-citizen-lab/#:%7E:text=The%20list%20of%20mercenary%20spyware,Cyberbit%2C%20Circles%2C%20and%20Cytrox.

Manancourt, V. (2022a, juni 21). *Pegasus makers face EU grilling. Here's what to ask them*. POLITICO. Geraadpleegd op 11 juli 2022, van https://www.politico.eu/article/pegasus-makers-testify-in-eu-parliament-heres-what-to-ask-them/

Mazzetti, M., & Bergman, R. (2022, 11 juli). *Defense Firm Said U.S. Spies Backed Its Bid for Pegasus Spyware Maker*. The New York Times. Geraadpleegd op 11 juli 2022, van https://www.nytimes.com/2022/07/10/us/politics/defense-firm-said-us-spies-backed-its-bid-for-pegasus-spyware-maker.html

O'Neill, P. H. (2019, 28 februari). *ISS World: The traveling spyware roadshow for dictatorships and democracies*. CyberScoop. Geraadpleegd op 11 juli 2022, van https://www.cyberscoop.com/iss-world-wiretappers-ball-nso-group-ahmed-mansoor/

O'Neill, P. H. (2020, 9 november). *Europe is adopting stricter rules on surveillance tech*. MIT Technology Review. Geraadpleegd op 11 juli 2022, van https://www.technologyreview.com/2020/11/09/1011837/europe-is-adopting-stricter-rules-on-surveillance-tech/

O'Neill, P. H. (2022, 27 juni). *The hacking industry faces the end of an era*. MIT Technology Review. Geraadpleegd op 11 juli 2022, van

https://www.technologyreview.com/2022/06/27/1054884/the-hacking-industry-faces-the-end-of-an-era/

The Pegasus Spyware Could Be Stealing Your Data. . . (2021, 20 juli). [Video]. YouTube. https://www.youtube.com/watch?v=qEB6X4yJCXA&ab_channel=SomeOrdinaryGamers

OPERATING IN THE SHADOWS. (2021). Amnesty International.

Privacy International. (2016, juli). *The Global Surveillance Industry*.

Rethinking How We Talk about Spyware Regulation. (2022, 8 juni). Leiden Security and Global Affairs Blog. Geraadpleegd op 11 juli 2022, van https://www.leidensecurityandglobalaffairs.nl/articles/rethinking-how-we-talk-about-spyware-regulation

Roussi, A. (2022, 22 juni). *Pegasus used by at least 5 EU countries, NSO Group tells lawmakers*. POLITICO. Geraadpleegd op 11 juli 2022, van https://www.politico.eu/article/pegasus-use-5-eu-countries-nso-group-admit/

Taming Pegasus: A Way Forward on Surveillance Tech Proliferation. (2020). Privacy International. Geraadpleegd op 11 juli 2022, van https://privacyinternational.org/news-analysis/4602/taming-pegasus-way-forward-surveillance-tech-proliferation

TechCrunch is part of the Yahoo family of brands. (2022a, februari 15). TechCrunch. Geraadpleegd op 11 juli 2022, van https://techcrunch.com/2022/02/15/eu-data-protection-pegasus/

TechCrunch is part of the Yahoo family of brands. (2022b, maart 11). TechCrunch. Geraadpleegd op 11 juli 2022, van

https://techcrunch.com/2022/03/11/europe-pegasus-investigation/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKOITmFm70i-Belh5VV8HVJfUFtltW8xY5IWmCbQLd1w2oKQK-dsPxbjm-HHr4Nu866Uje0lwjzpVo9QOAW_6XIQctYTCoXFXTr7DUM3veHwWpectreF71wvWHrs8dGExAONiZJqwljJDZnb3bMt7S3WPzCvYHvV4kC-cbh_sk1X

Westbroek, D. B. B. (2022, 19 april). *Recast of the EU Dual-Use Regulation set to enter into force on 9 September 2021*. De Brauw Blackstone Westbroek. Geraadpleegd op 11 juli 2022, van https://www.debrauw.com/articles/recast-of-the-eu-dual-use-regulation-set-to-enter-into-force-on-9-september-2021