Skyline successfully launches a campaign to stop spying software Pegasus

Skyline International for Human Rights (SIHR) has officially launched its campaign, aiming to stop the commercial use of the spying software Pegasus, developed by Israeli company NSO Group. According to an investigation carried out by Citizen Lab and the French based organization Forbidden Stories, this technology has been used to facilitate violations and crimes against freedom of expression and human rights on an unprecedented scale.

During its presentation at the event, Daniel Rivera, Skyline Director, mentioned that this technology was supposedly created to fight against terrorism. Still, the truth is that hundreds if not thousands of journalists, activists, heads of state, and other professionals and their families have been targeted by intelligence services around the MENA region using this technology. 1

Skyline International for Human rights believes it is crucial to stop this technology from spreading and being commercialized around the world without a clear legal framework regulating its usage. Skyline has sent A joint letter to the United Nations High Commission on Human Rights to condemn Pegasus and urge to take action against countries that used NSO Group's spyware to hack the phones of human rights activists, journalists and actors/individuals.

SIHR has invited leading experts in human rights and surveillance technology to increase social awareness and explain to the public the dangers of this growing industry.

Marwa Fatafta, policy manager at Access Now, began her intervention by explaining the origins of this technology and how it works. Pegasus is a spy software developed by the the Israeli company NSO Group created in 2010. It can infect your phone and extract all the information placed within the device: email, messages, photos, pictures. In addition, it can access the camera and audio, among other functions of your device that can be remotely manipulated. All this information is extracted and send it to a client who is interested in spying on you. As Marwa mentioned: "indeed turns your phone into a spying device."

Marwa also explained how a device could be infected. It could be infected through a malicious link send to the target, tricks the person to give access to his device through an invitation. For instance, she mentioned the Emirate human rights activist, Ahmed Mansour, who received a link supposedly with updates and news about human rights issues in the UAE and invited him to click on the link. Also, there is the case of a Saudi human rights activist in Canada who received a link looking as a DHL shipping tracking notice, but once you click on the link, your computer gets infected.

However, there is another way to infect a device without the need for users to do anything. This attack is called a "zero-click" attack, and in this case, there is no need for any interaction with the device owner. To achieve this, NSO Group exploits the vulnerabilities in your device. So regardless of how careful you are, there is anything you can do to stop this kind of attack.

Marwa points out that after the investigation done by several organizations, we can conclude that Pegasus has been used by authoritarian and democratic governments alike to target activists, human rights advocates, journalists, lawyers, and civil society actors. NSO Group claims that only sales this technology to vetted governments and refuses to sell to governments violating human rights.

However, the investigation revealed that most of the NSO Group clients are accused of human rights violations, especially among its clients in the MENA region: Morocco, UAE, Saudi, Bahrain, to name a few. The NSO Group has been profiting from human rights violations worldwide with little accountability and transparency on its operations, and we believe the revelations of the investigation are just the tip of the ice-berg. So far, we don't know the full list of clients of NSO Group, in terms of human rights abuses, and targets.

The Gulf Center for Human Rights' executive director, Khalid Ibrahim, talked about the cooperation between the NSO Group and oppressive governments in the MENA region. He explained the impact on the peaceful and legitimate work of human rights defenders and what we should do to enhance the protection of HRDs in the face of such cooperation. Khalid underlined the importance of this campaign to stop companies such as NSO Group. He stated: "*This technology is profoundly affecting the community of human rights defenders in the MENA region. It is vital to stop this cooperation between the NSO and other groups alike with aggressive governments in the MENA region and elsewhere.*" Then, he added: "Precisely, Ahmed Mansoor is an example of how this technology is being used in the MENA region."

Khaled continued explaining about this case: "in 2021, several human rights organization such as HRW and the GCHR resealed a report entitled: "United Arab Emirates: Prominent Jailed Activist in Danger,"[1] and we know Amed Mansoor was there, who was a victim of Pegasus, and who has been in jail for 10 years based on many fabricated charges related to his activities as human rights advocate, and for collaborating with organizations such as Amnesty International, Human Rights Watch, and the Gulf Center for Human Rights among others. We also know that the UAE expended millions to acquire all this information from Mansoor before his arrest in March 2017."

Also, Khaled mentioned that the EU parliament passed a resolution this September calling for his release. Moreover, the GCHR is collaborating closely with the EU to prevent such

[1] United Arab Emirates: Prominent Jailed Activist in Danger. GCHR. 19.07.21. <https://www.gc4hr.org/news/view/2786>. Also, Skyline calls for monitoring detainees' conditions in the UAE prisons. Skyline International for Human Rights. 25 JUL 2021. <https://skylineforhuman.org/en/news/details/446/skyline-calls-for-monitoring-detainees-conditions-in-the-uae-prisons>

cooperation between the NSO Group and members of the EU. Nevertheless, another issue that we tend to forget mentioned Khaled is that usually this technology affects not only the

targeted person but also people closely related to him, such as family members, friends, and colleagues. This is why is so important to stop this collaboration.

Khalid stressed that their work as human rights organization is at risk. For instance, Marwa mentioned some of the countries using this technology in the Gulf, such as Saudi Arabia, UAE, and Bahrain. Still, recently we could add to the list Oman, who has passed a piece of legislation last year authorizing the internal security service unlimited access to the internet activities in the country. Basically, the Oman security forces control the internet in their country. Furthermore, the government allows the internal security service to import the most sophisticated surveillance equipment and advanced technology to monitor online actives in the internet.

Another business emerging from this industry is that these countries can now offer some of these services to other countries that do not have access or resources to acquire this technology, spreading its usage in every corner of the MENA region. Marwa mentioned that this problem goes beyond the NSO Group since an industry is emerging between private digital mercenaries and the states interested in using this technology to target activists and human rights defenders. The NSO Group has become the embodiment of this emerging industry.

There is a huge surveillance industry that operates in the dark, without accountability, and is profiting, engaging and facilitating human rights abuses and violations through the sales and transfer of this technology. According to Microsoft, the surveillance industry represents a $12 billion dollar industry today. For instance, we know the UAE was importing technology and contractors to work in surveillance projects in the UAE, targeting not only their citizens but also prominent foreign figures in the case known today as Trident. We don't know much about it, but Access now and others organizations are working to shed light on the actives of this emerging industry.

Sherif Mansour, the Middle East and North Africa Coordinator at Committee for Protecting Journalist CPJ talked about journalists' impact, including those online and exiled. Will also give examples on those covering corruption in Morocco and my personal experience documenting elections fraud in Egypt.

Morocco is important because many journalists have been affected by spyware and a combination of legal actions and other tactics such as smear campaigns and physical assaults, hampering their ability to investigate corruption cases. This is at the heart of the problem. Privacy is crucial to be able to conduct their job, to contact sources and publish critical information. According to CPJ's research, journalists who work online and usually abroad are especially vulnerable to these attacks.

Also, their family members and colleagues are usually affected. The case of Jamal Khashoggi is an example, before and after his assassination, his associates and family members were

spied on. And it is not just about mourning the death of someone you loved. This situation takes a tremendous psychological toll on victims seeking accountability because they feel this

technology also targeted them. As a result, many journalists have expressed significant concern regarding the lack of privacy, and they are more conscious about their work and what their write, knowing they could become a target.

Sharif pointed out that according to CPJ's investigation, 17 States have been involved in activities persecuting activities abroad. For example, Khashoggi was an exiled journalist. Many others like him, who could not keep publishing in their countries because their publications were shut, had the internet as their only venue to public their work. It is then when states decide to go the extra mile and persecute them using this technology. According to Sherif: *"Therefore the response should not be local, regional but international."*

Then, he added: "This is why the CPJ has sent a recommendation to the United States, European Union, and the United Nations officials to work together. Now we have 160 organizations worldwide calling on a moratorium in the experts of surveillance software. Also, CPJ supports the lawsuit in the United States filled by WhatsApp and other companies using NSO Group to infiltrate and breach the privacy in their software." So, there are growing public and private sector concerns about the effects of this technology in their platforms. Sharif explained that once they have access to your phone, they can access any application of your phone as well regardless of the encryption of the messaging apps such as signal, messenger, or WhatsApp.

It is clear for all the guests in this event that spying technology has been used to enhance repression against dissident voices beyond national borders. Now, exiled journalists in the MENA can't even feel safe as exiles, where traditionally dissidents could find more protection. This technology enhances censorship and repression beyond the borders of regimes famous for violating human rights and freedom of expression.

The only thing left to ask is what we can do to protect ourselves against this technology. According to Khalid, it is essential to be sure your phone has not been infected with the help of an IT expert. Also, it's impossible to file a local complaint about this matter or protect the victims, so it is essential to use the concept of international jurisdiction and take the battle to internationally recognized courts, which can take legal action at the international level. The GCHR, in collation with other organizations, has recently participated in legal case presented in France against the NSO Group. More and more groups are joining these efforts to isolate NSO, and I believe more international organizations and states should join the effort.

Marwa pointed out that there are several venues that must be explored to stop Pegasus. First, we need to do a full and global investigation to understand the scoop and reach of this technology. Also, we need to think about remedies for the victims.

Also, we need to create international and national legislation to ensure that companies such as this have to disclose their clients and operations, so we can be sure human rights provisions

are contemplated. However, it can be argued that this technology by definition violates human rights, and there is no way states can respectfully use Pegasus. Also, we need to act in different jurisdictions and make sure national laws also regulate the industry. Therefore

litigation is a way to keep presuming and isolating companies such as this. As a summary: "*accountability through litigation, regulation both global and national, and having robust exports control on surveillance technology*" are the main issues to focus on, according to Marwa.

Finally, Sharif mentioned that it is paramount to remember that no one is safe with this technology, although NSO Groups claim that US phones can't be hacked. Unfortunately, there is no way of knowing if this is true. So, it is important to remember that not only Israeli companies, but European and American, as well as other companies in Israel that are not Pegasus, are profiting from this technology.

The EU has taken some accountability measures by establishing some expert control on this technology, and we expect the US to do the same soon. Also, we expect the US that can establish strict controls over its companies will do the same pressure its allies to do the same (Morocco, Israel, Saudi, UAE), which are selling, investing and profiting this technology. Investigating and reporting these abuses by the US government would help emphasizes the work of civil society and the general public on this issue.

In summary, it is paramount to continue pressuring states, international organizations, and the public to stop commercializing this kind of technology that flagrantly violates human rights and freedom of expression. This technology weaponizes civilian technology, turns it against its users, causing tremendous damage to his work, private life, and reputation. Today, our guests have shown the dangers of this software and industry and what we must do to stop this spy software from spreading worldwide.