



Silent Intruders:

Navigating the Intersection of Modern Spyware tools and Fundamental Rights

A European Perspective

Guns don't kill people,
people kill people.

Michael Moore

 quote fancy

Geraldine Noel
Barrister – England & Wales, Ireland, Malta
M.A(Hons)(Oxford), Pg Dip (London), LLM (Fordham)

NEWS > CYBERSECURITY AND DATA PROTECTION

Brussels spyware crisis expands: Two MEPs hit in phone-hacking security breach

Lawmakers found malware infections on their phones, ringing alarm bells about confidential EU defense work.

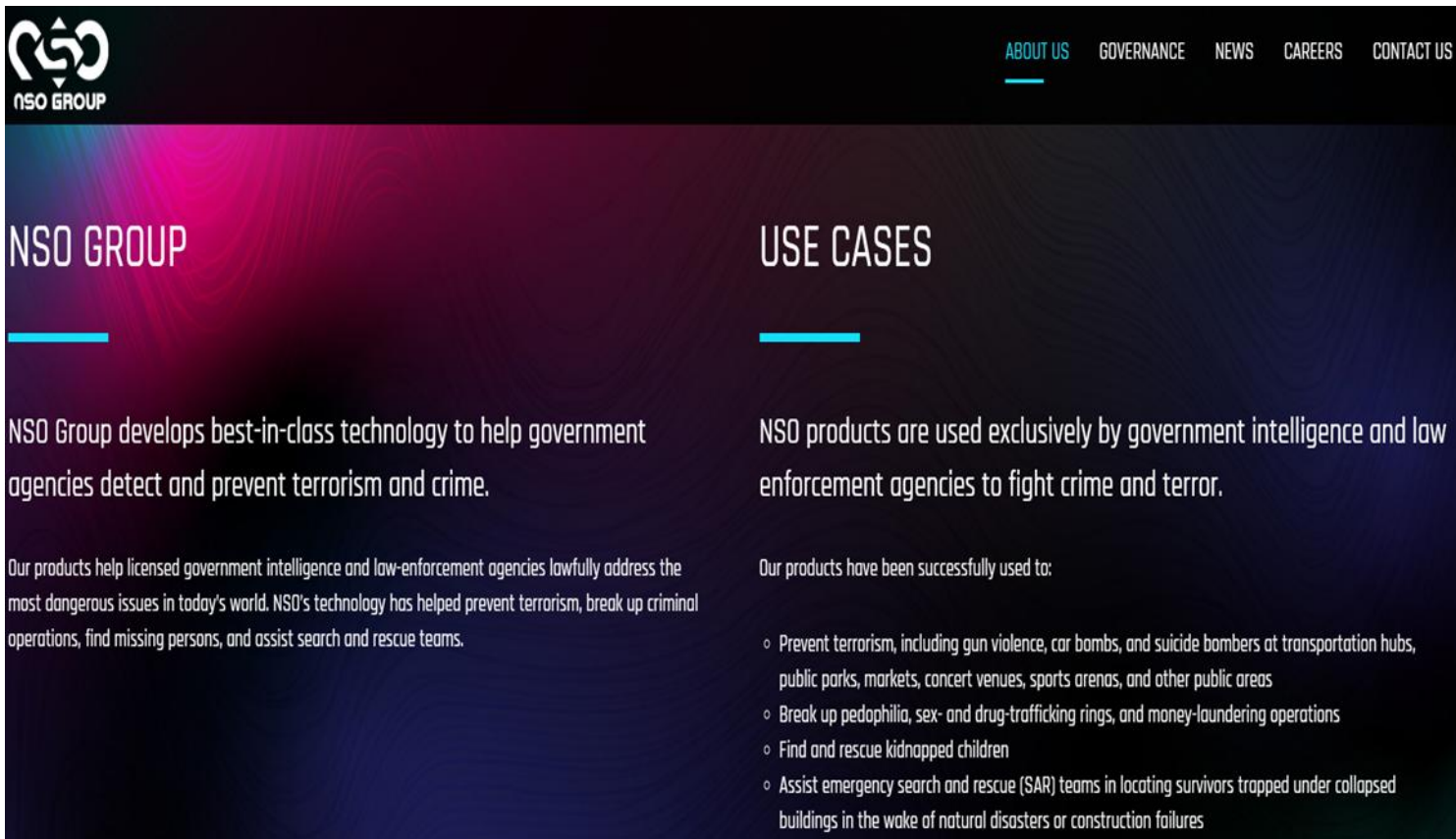
FEBRUARY 22, 2024 2:23 PM CET

‘The Pegasus software was developed by the Israeli NSO Group and has been used to breach mobile phones and extract data stored or processed by the target system, including text messages, call interceptions, locations, and information from apps.’

EPRS | European Parliamentary Research Service

Author: CosticaDumbrava, Members' Research Service

PE 747.923 –June 2023



The screenshot shows the NSO Group website. The header includes the NSO GROUP logo and navigation links: ABOUT US, GOVERNANCE, NEWS, CAREERS, and CONTACT US. The main content area is divided into two columns. The left column, titled 'NSO GROUP', states: 'NSO Group develops best-in-class technology to help government agencies detect and prevent terrorism and crime.' and 'Our products help licensed government intelligence and law-enforcement agencies lawfully address the most dangerous issues in today's world. NSO's technology has helped prevent terrorism, break up criminal operations, find missing persons, and assist search and rescue teams.' The right column, titled 'USE CASES', states: 'NSO products are used exclusively by government intelligence and law enforcement agencies to fight crime and terror.' and 'Our products have been successfully used to:' followed by a bulleted list of use cases.

NSO GROUP

NSO Group develops best-in-class technology to help government agencies detect and prevent terrorism and crime.

Our products help licensed government intelligence and law-enforcement agencies lawfully address the most dangerous issues in today's world. NSO's technology has helped prevent terrorism, break up criminal operations, find missing persons, and assist search and rescue teams.

USE CASES

NSO products are used exclusively by government intelligence and law enforcement agencies to fight crime and terror.

Our products have been successfully used to:

- Prevent terrorism, including gun violence, car bombs, and suicide bombers at transportation hubs, public parks, markets, concert venues, sports arenas, and other public areas
- Break up pedophilia, sex- and drug-trafficking rings, and money-laundering operations
- Find and rescue kidnapped children
- Assist emergency search and rescue (SAR) teams in locating survivors trapped under collapsed buildings in the wake of natural disasters or construction failures

Number of attendees at arms fairs and ISSWorld marketing spyware capabilities demonstrates the prevalence of third country providers of spyware and related products and services, a significant number of which are headquartered in:

Israel - NSO Group, Wintego, Quadream and Cellebrite

India - ClearTrail

United Kingdom - BAe Systems and Black Cube

United Arab Emirates – DarkMatter

Russia - Positive Technologies

Singapore - Computer Security Initiative Consultancy PTE LTD.

further highlights the diversity of origin among spyware producers; whereas the fair is also attended by a wide range of European public authorities, including local police forces

Investigation of the use of Pegasus and equivalent surveillance spyware

Following revelations that several EU governments used the Pegasus spyware software against journalists, politicians, officials and other public figures, the European Parliament set up a Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA). Parliament is set to hold a debate on PEGA's findings and vote on a recommendation to the Council and Commission during the June 2023 session.

Background

In 2021, several [civil society organisations](#) and investigative journalists started to reveal that government bodies in several countries, both EU Member States and non-EU countries, had used Pegasus and equivalent surveillance spyware against journalists, politicians, law enforcement officials, diplomats, lawyers, business people, civil society actors and others, for political and even criminal purposes. The Pegasus software was developed by the Israeli NSO Group and has been used to breach mobile phones and extract data stored or processed by the target system, including text messages, call interceptions, locations, and information from apps. The use of Pegasus and equivalent surveillance spyware poses a [threat](#) to the fundamental rights guaranteed under the [Charter of Fundamental Rights of the EU](#) (such as the right to privacy and data protection, freedom of expression, freedom of the press, and freedom of association) and the principles contained in the [Treaties](#) (such as democracy and the rule of law). The proliferation and abuse of spyware also raises issues about the effectiveness of EU [export controls](#), human rights safeguards in the [procurement of spyware](#) from third countries, and foreign policy cooperation.

European Parliament position

On 8 March 2023, the [PEGA committee](#) adopted a [report](#) on its investigation on the use of Pegasus and equivalent spyware software. Based on this report, the rapporteur has prepared a recommendation to the Council and the Commission. Subject to final compromise, the [draft recommendation](#) of 22 May 2023 strongly condemns the illegitimate use of spyware by Member State governments or members of government. It concludes that there is evidence of degrees and forms of contravention and maladministration of EU law in Poland, Hungary, and Greece. It finds deficits in the implementation of the EU Dual-use Regulation in Cyprus and notes a need for reform in Spain. It also states that 'it can be safely assumed that all Member States have purchased or used one or more spyware systems'. According to the draft recommendation, there were serious shortcomings in the implementation of Union law when the Commission and the European External Action Service provided support to non-EU countries to enable them to develop surveillance capabilities. As stated in the draft text, Parliament considers that there is 'a clear need for common EU standards regulating the use of spyware by Member State bodies'. The draft underlines the need for better enforcement of EU law, including data protection law, the Anti-Money-Laundering Directive, procurement rules, the Dual-use Regulation, and the Whistleblower Directive, to counter deficiencies in national legislation. It also calls for additional European legislation requiring corporate actors producing and/or exporting surveillance technologies, to include human rights and due diligence frameworks.

Own-initiative procedure: [2022/2077\(INI\)](#); Committee responsible: LIBE; Rapporteur: Sophia in 't Veld (Renew, the Netherlands). For further information see [EPRS study](#).

EPRS | European Parliamentary Research Service

Author: Costica Dumbrava, Members' Research Service

PE 747.923 – June 2023



This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy. © European Union, 2023

eprs@ep.europa.eu (contact) <http://www.eprs.ep.parl.union.eu> (intranet) <http://www.europarl.europa.eu/thinktank> (Internet) <http://eprthinktank.eu> (blog)

The Charter of Fundamental Rights of the European Union

- right to privacy and data protection
- freedom of expression
- freedom of the press
- freedom of association
- respect for private and family life
- protection of personal data
- freedom of expression and information
- right to property, right to non-discrimination
- right to effective remedy and fair trial
- whereas it results from the testimonies of victims that even if legal remedy and civil rights may exist on paper, they mostly become void in the face of obstruction by government bodies, the absence of implementation of the right to be informed for victims and the administrative burden to prove the status as victim; I. whereas the Polish government has weakened and eliminated institutional and legal safeguards including proper oversight and scrutiny procedures, effectively leaving victims without any meaningful remedy; whereas the Pegasus surveillance spyware has been illegally deployed to spy on journalists, politicians, prosecutors and civil society actors for political purposes;

Doc. 15825 20 September 2023
Pegasus and similar spyware and secret state surveillance Report Committee on
Legal Affairs and Human Rights
Rapporteur: Mr Pieter OMTZIGT, Netherlands, Group of the European People's Party

In July 2021, an international coalition of investigative journalists coordinated by Forbidden Stories, with the technical support of Amnesty International's Security Lab ("the Pegasus Project"), published information about a leaked list of over **50,000 phone numbers** identified as potential targets by clients of NSO Group, an Israeli company that developed and globally markets a spyware called Pegasus.

This list included **human rights defenders**, political opponents, **lawyers**, diplomats, Heads of State and nearly **200 journalists** from **24 countries**.

11 countries around the world were identified as potential NSO clients, including two Council of Europe member States, Azerbaijan and Hungary. And **at least 14 European Union countries**, including Belgium, Germany (in a modified version), Hungary, Luxembourg, the Netherlands, Poland and Spain.

EUROPEAN PARLIAMENT DRAFT RECOMMENDATION TO THE COUNCIL AND THE COMMISSION pursuant to Rule 208(12) of the Rules of Procedure following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware

Sophie in 't Veld on behalf of the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware
04.01.2023

Recommendations:

Charter of Fundamental Rights of the European Union (the 'Charter'), and in particular Articles 7, 8, 11, 17, 21 and 47 thereof,

EU regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items – bypassed by Cyprus & Bulgaria

1 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Charter of the United Nations and the United Nations Guiding Principles on Business and Human Rights¹⁰,

European Convention for the Protection of Human Rights and Fundamental Freedoms, and in particular Articles 8, 9, 13 and 17 thereof, and the Protocols to that Convention

EPRS | European Parliamentary Research Service Author: Hendrik Mildebrath Members' Research Service PE 766.262 – November 2024

- Country-specific recommendations for these Member States.
- Stronger institutional and legal safeguards to ensure fundamental rights-compliant use of spyware by law enforcement. It
- Development of strict spyware surveillance standards that include conditions for ordering, authorising, executing, and overseeing spyware operations, along with requirements for effective redress.
- Parliament acknowledges that surveillance operations for national security purposes in principle remains the exclusive competence of Member States, but points out that EU law regulates certain national security surveillance activities indirectly.
- Surveillance in the name of national security should be the exception rather than the rule in a democratic transparent society. Additionally, Parliament proposes to limit the circulation of commercial spyware on the EU market to spyware designed in line with its envisaged spyware standards ('rule of law by design').
- Proposal to limit the circulation of commercial spyware on the EU market to spyware designed in line with its envisaged spyware standards ('rule of law by design').
- Permitting the sales of functionally compliant spyware technologies, it recommends prohibiting 'hacking as a service', including technical, operational and methodological support.
- Tasked the Commission with drafting new laws as proposed by Parliament, notably regulating EU spyware surveillance standards and the placing of spyware on the market

However:

Parliament recommends regulating the use of spyware for law enforcement based on the Treaty provisions relating to judicial cooperation in criminal matters (Chapter 4 of Title 5 of the Treaty on the Functioning of the European Union, TFEU). Under this approach, qualified surveillance operations and frameworks would become subject to EU spyware standards, **while national security operations would, at best, be regulated indirectly by EU data protection and privacy rules, and – in most cases – remain entirely outside the scope of application of EU law.**

What can be done?

NGOs

- Center for Democracy & Technology (CDT)
<https://cdt.org/>
- Renew Europe
<https://www.reneweuropengroup.eu/campaigns/pegasus>



Think Tanks

- European Union Think Tank
<https://esthinktank.com/2022/05/25/the-changes-in-the-law-that-pegasus-is-forcing-on-the-eu/>
- European Parliament Think Tank
<https://epthinktank.eu/2024/06/02/what-action-has-parliament-taken-against-spyware-abuse/>



Objectives

- Ensure individuals' personal information is secure from unwarranted and disproportionate government surveillance and law enforcement overreach, particularly in the context of national security and public order measures.
- Promote government accountability and robust checks and balances to safeguard fundamental rights in online spaces.
- Ensure the development, use and protection of strong encryption technologies to safeguard communications and data from unauthorised access, including disproportionate surveillance on grounds of national security.
- Strengthening spyware regulation to prevent abuse and protect fundamental rights.
- Ensuring a rights-compliant data retention framework that safeguards privacy.
- Promoting encryption as a key tool for secure and private communications

COMMONWEALTH
LAW CONFERENCE 2025

6th – 10th April



Thank You

Geraldine Noel
Barrister – England & Wales, Ireland, Malta

gnoel@acumum.com