European Parliament
2019-2024

Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware

2022/2077(INI)

30.1.2023

AMENDMENTS
1021 - 1281

Draft report
Sophia in 't Veld
(PE738.492v03-00)

Investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware
(2022/2077(INI))

Amendment 1021
Cornelia Ernst, Stelios Kouloglou, Giorgos Georgiou, Anne-Sophie Pelletier

Motion for a resolution
Paragraph 142 b (new)

Motion for a resolution	*Amendment*
	142 b. Multiple reports by Amnesty International have revealed that targeted attacks using NSO's Pegasus spyware have been ongoing since at least 2017. The targets include Maati Monjib, an academic and activist working on issues of freedom of expression and Abdessadak El Bouchattaoui, a human rights lawyer and activist.[286a] In 2019, Omar Radi, a prominent journalist and activist from Morocco was also targeted[286b], and in July 2021, the case of Moroccan journalist in exile Hicham Mansouri and Claude Mangin, partner of a Sahraoui activist.

286a

https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-

286b

https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/

Or. en

Amendment 1022
Sophia in 't Veld

Motion for a resolution
Paragraph 142 c (new)

Motion for a resolution	*Amendment*
	142 c. In July 2017, Circles Bulgaria EOOD - another NSO subsidiary - registered in Sofia with the Cypriot CS-

Circles Solutions Ltd. as parent company. The main activities of Circles Bulgaria are described as 'Computer Systems Design and Related Services'. The company employs 147 people at the time of writing[1a].

[1a] EMIS. Circles Bulgaria EOOD.

Or. en

Amendment 1023
Cornelia Ernst, Stelios Kouloglou, Giorgos Georgiou, Anne-Sophie Pelletier

Motion for a resolution
Paragraph 142 c (new)

Motion for a resolution	*Amendment*
	142 c. Western Sahara is the subject of a territorial dispute between Morocco, which annexed the territory in 1975 and claims sovereignty over it, and the Polisario Front, which calls for an independent state in the territory and has set up a government-in-exile in the refugee camps in Tindouf, south-west Algeria

Or. en

Amendment 1024
Saskia Bricmont, Hannah Neumann, Diana Riba i Giner, Jordi Solé, Gwendoline Delbos-Corfield, Marcel Kolaja

Motion for a resolution
Paragraph 142 c (new)

Motion for a resolution	*Amendment*
	142 c. In July 2017, Circles Bulgaria EOOD - another NSO subsidiary - registered in Sofia with the Cypriot CS-Circles Solutions Ltd. as parent company. The main activities of Circles Bulgaria

are described as 'Computer Systems Design and Related Services'. The company employs 147 people at the time of writing.

Or. en

Amendment 1025
Sophia in 't Veld

Motion for a resolution
Paragraph 142 d (new)

Motion for a resolution	*Amendment*
	142 d. According to the Public Register of Persons Registered for Export and Transfer of Dual-Use Items and Technologies as provided for by the Bulgarian Ministry of Economy, both NSO subsidiaries Magnet Bulgaria and Circles Bulgaria have received export licenses. Magnet Bulgaria received an export license that expired on 12 May 2020[1a]. Based on a letter sent by NSO to Amnesty International, Magnet Bulgaria is dormant at time of writing[1b]. Circles Bulgaria is currently still active and has received an export license that is valid until 25 April 2023[1c]. Whereas NSO Group subsidiaries have received export licenses from the Bulgarian authorities, the Bulgarian government denies the granting of export licenses to NSO group itself[1d].

[1a] https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.mi.government.bg%2Ffiles%2Fuseruploads%2Ffiles%2Fexportcontrol%2Fregistar_iznos_transfer_22112018.xls&wdOrigin=BROWSELINK

[1b] Amnesty International. Operating From the Shadows: Inside NSO Group's Corporate Structure.

1c

https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.mi.government.bg%2Ffiles%2Fuseruploads%2Ffiles%2Fexportcontrol%2Fregistar_iznos_transfer_22112018.xls&wdOrigin=BROWSELINK

1d ***Access Now. Is NSO Group's infamous Pegasus spyware being traded through the EU?***

Or. en

Amendment 1026
Saskia Bricmont, Hannah Neumann, Diana Riba i Giner, Jordi Solé, Gwendoline Delbos-Corfield, Marcel Kolaja

Motion for a resolution
Paragraph 142 d (new)

Motion for a resolution	*Amendment*
	142 d. According to the Public Register of Persons Registered for Export and Transfer of Dual-Use Items and Technologies as provided for by the Bulgarian Ministry of Economy, both NSO subsidiaries Magnet Bulgaria and Circles Bulgaria have received export licenses. Magnet Bulgaria received an export license that expired on 12 May 2020. Based on a letter sent by NSO to Amnesty International, Magnet Bulgaria is dormant at time of writing. Circles Bulgaria is currently still active and has received an export license that is valid until 25 April 2023. Whereas NSO Group subsidiaries have received export licenses from the Bulgarian authorities, the Bulgarian government denies the granting of export licenses to NSO group itself.

Or. en

Amendment 1027
Cornelia Ernst, Stelios Kouloglou, Giorgos Georgiou, Anne-Sophie Pelletier

Motion for a resolution
Paragraph 142 d (new)

Motion for a resolution	*Amendment*
	142 d. In July 2021, it was reported that Israel and Morocco signed their first-ever cyber defence deal just six months after the announcement of the normalisation deal.[282a]
	[282a] https://www.google.com/url?q=https://www.jpost.com/israel-news/israel-morocco-ties-strengthen-with-signing-of-first-cyber-defense-deal-674089&sa=D&source=docs&ust=1674664016238766&usg=AOvVaw2K7ZNS6VHBCaQx0gf_Rbqe

Or. en

Amendment 1028
Sophia in 't Veld

Motion for a resolution
Paragraph 142 e (new)

Motion for a resolution	*Amendment*
	142 e. The Sofia City Prosecutor's Office has started an investigation to inquire if the Pegasus Spyware has been illegally used by Bulgarian government entities. This inquiry is ongoing at the time of writing[1a].
	[1a] BNR. Sofia City Prosecutor's Office investigates possible use of Pegasus spyware in Bulgaria; European Parliament. Pegasus and surveillance spyware.

Or. en

Amendment 1029
Saskia Bricmont, Hannah Neumann, Diana Riba i Giner, Jordi Solé, Gwendoline Delbos-Corfield, Marcel Kolaja

Motion for a resolution
Paragraph 142 e (new)

Motion for a resolution	*Amendment*
	142 e. The Sofia City Prosecutor's Office has started an investigation to inquire if the Pegasus Spyware has been illegally used by Bulgarian government entities. This inquiry is ongoing at the time of writing.

Or. en

Amendment 1030
Cornelia Ernst, Stelios Kouloglou, Giorgos Georgiou, Anne-Sophie Pelletier

Motion for a resolution
Paragraph 142 f (new)

Motion for a resolution	*Amendment*
	142 f. Israel
	The Israeli government is at the centre of the spyware market as the leaders allegedly use the spyware as a diplomatic bargaining chip in pursuit of various foreign policy objectives. As with the export of weapons systems, Israel's defense ministry must approve all foreign sales of Pegasus and thus plays a critical oversight role in its proliferation. According to the Israeli government, such exports are says it authorized licenses according to the Wassenaar Arrangement's guidelines on preventing malign actors from accessing products that could be used for illicit purposes; it has also said its export decisions are made "in accordance with diverse

considerations," including human rights. However, some unnamed Israeli officials reportedly said that Israel's foreign policy interests outweighed human rights concerns.[283a]

283a

https://www.google.com/url?q=https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate&sa=D&source=docs&ust=1674664016227987&usg=AOvVaw2XNJ0FI7xUBa0tNkhvbKcZ

Or. en

Amendment 1031
Cornelia Ernst, Stelios Kouloglou, Giorgos Georgiou, Anne-Sophie Pelletier

Motion for a resolution
Paragraph 142 h (new)

Motion for a resolution	*Amendment*
	142 h. It should also be noted that surveillance technology in Israel is designed and implemented in the context of the Israeli military operation to uphold a system of multilayered control and oppression. The abuse of spyware technologies by Israel can be seen by the control and repression of Palestinian people. According to the report by the Front Line Defenders, in October 2021, which has been confirmed by CitizenLab and Amnesty International, six Palestinian human rights defenders were hacked with Pegasus, out of which two are dual-national: one French, the other American.[284a]

284a

https://www.google.com/url?q=https://citizenlab.ca/2021/11/palestinian-human-rights-defenders-hacked-nso-groups-pegasus-

spyware/&sa=D&source=docs&ust=1674664016231837&usg=AOvVaw2OXYwCwCot44nq0t-F55DY

Or. en

Amendment 1032
Sophia in 't Veld

Motion for a resolution
Paragraph 143 a (new)

Motion for a resolution	*Amendment*
	143 a. According to the Commission's response to the PEGA committee on 9 September 2022[1a], these checks did not confirm any compromise of Commissioner Reynders's personal or professional device, "neither ... before or after this date [23 November]". The Commission's competent services also inspected devices of additional staff who received similar notifications from Apple on the same day, but "none of the inspected devices confirmed Apple's suspicions" either.

[1a] Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022

Or. en

Amendment 1033
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 143 a (new)

Motion for a resolution	*Amendment*
	143 a. According to the Commission's

response to the PEGA committee on 9 September 2022, these checks did not confirm any compromise of Commissioner Reynders's personal or professional device, "neither ... before or after this date [23 November]". The Commission's competent services also inspected devices of additional staff who received similar notifications from Apple on the same day, but "none of the inspected devices confirmed Apple's suspicions" either.

Or. en

Amendment 1034
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 143 b (new)

Motion for a resolution	*Amendment*
	143 b. However, in letters of 25 July 2022 and 9 September 2022, the Commission acknowledged that in the course of the ongoing investigation into the targeting of the Commission with Pegasus, "several device checks led to the discovery of indicators of compromise." The Commission has so far refused to further elaborate on the investigation's findings, as "they would reveal to adversaries the Commission's investigation methods and capabilities, thus seriously jeopardizing the institution's security."Unofficial reports of more than fifty detected infections have not been confirmed by the Commission. Despite multiple invites by the PEGA Committee, the Commission has refused to share further information on the number of departments subject to the compromise, profession of staff or any further information that would be of interest to the PEGA Committee's work and could determine the origin of the

attack.

Or. en

Amendment 1035
Sophia in 't Veld

Motion for a resolution
Paragraph 143 b (new)

Motion for a resolution	*Amendment*
	143 b. However, in letters of 25 July 2022 and 9 September 2022, the Commission acknowledged that in the course of the ongoing investigation into the targeting of the Commission with Pegasus, "several device checks led to the discovery of indicators of compromise." The Commission has so far refused to further elaborate on the investigation's findings, as "they would reveal to adversaries the Commission's investigation methods and capabilities, thus seriously jeopardizing the institution's security."[1a] Unofficial reports of some sixty detected infections have not been confirmed by the Commission.
	[1a] Response letter by Commissioners Hahn and Reynders to the rapporteur - 25 July 2022; Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022

Or. en

Amendment 1036
Sophia in 't Veld

Motion for a resolution
Paragraph 143 c (new)

Motion for a resolution	*Amendment*

143 c. On 15 July 2022 the PEGA committee asked the Commission whether it requested the assistance of Citizen Lab for its investigation. However, the Commission did not deem it necessary to follow up further, and stated that "the information made publicly available by Citizens Lab and Amnesty International did not allow to confirm that Commissioner Reynders's devices were infected by Pegasus"[1a], despite the fact that compromise was found on "several devices".

[1a] Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022

Or. en

Amendment 1037
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 143 c (new)

Motion for a resolution	*Amendment*
	143 c. On 15 July 2022 the PEGA Committee asked the Commission whether it requested the assistance of Citizen Lab for its investigation. However, the Commission did not deem it necessary to follow up further, and stated that "the information made publicly available by Citizens Lab and Amnesty International did not allow to confirm that Commissioner Reynders's devices were infected by Pegasus", despite the fact that compromise was found on "several devices".

Or. en

Amendment 1038
Sophia in 't Veld

Motion for a resolution
Paragraph 143 d (new)

Motion for a resolution	*Amendment*
	143 d. The Commission has declared that "Notifications of this kind are received multiple times on any given day by the Commission's relevant IT departments" and therefore they do not merit to be officially reported to the police. According to the Commission, since the Apple notification did not signal a "definitive infection, but the possibility of an attempt by the malware to target the corresponding device", the Commission did not follow up with law enforcement authorities[1a]. However, in contrast to the usual practice of non reporting, the Commission states that it "has been in contact with the Belgian police", on "technical details", as part of its "regular cooperation". It does not seem that the Commission officially reported the notifications or the "indicators of compromise" to the Belgian police for further investigation[1b]. This is remarkable. In other cases, for example Spain and France, a criminal investigation has been launched into the use of spyware against government ministers and heads of state. Spyware is used mainly by state actors, for reasons of national security. The Commission argues that "some aspects linked to national security fall outside the competences of the Commission", but it fails to explain how Commissioners and Commission staff would plausibly constitute a risk to national security.

[1a] Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022

[1b] Response letter by Commissioners Hahn and Reynders to the rapporteur - 25

July 2022

Or. en

Amendment 1039
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 143 d (new)

Motion for a resolution	*Amendment*
	143 d. The Commission has declared that "Notifications of this kind are received multiple times on any given day by the Commission's relevant IT departments" and therefore they do not merit to be officially reported to the police. According to the Commission, since the Apple notification did not signal a "definitive infection, but the possibility of an attempt by the malware to target the corresponding device", the Commission did not follow up with law enforcement authorities. However, in contrast to the usual practice of non reporting, the Commission states that it "has been in contact with the Belgian police", on "technical details", as part of its "regular cooperation". It does not seem that the Commission officially reported the notifications or the "indicators of compromise" to the Belgian police for further investigation. This is remarkable. In other cases, for example Spain and France, a criminal investigation has been launched into the use of spyware against government ministers and heads of state. Spyware is used mainly by state actors, for reasons of national security. The Commission argues that "some aspects linked to national security fall outside the competences of the Commission", but it fails to explain how Commissioners and Commission staff would plausibly

constitute a risk to national security.

Or. en

Amendment 1040
Dominik Tarczyński, Beata Kempa, Elżbieta Kruk
on behalf of the ECR Group

Motion for a resolution
Paragraph 144

Motion for a resolution	*Amendment*
144. According to the Commission, 'it is impossible to attribute these indicators to a specific perpetrator with full certainty.' The Commission holds that it cannot elaborate on the investigation's present-day findings, as 'they would reveal to adversaries the Commission's investigation methods and capabilities, thus seriously jeopardizing the institution's security'. ***The common, overarching topic that two of the known targeted Commission officials, Commissioner Reynders and a cabinet member of Commissioner Věra Jourová[284] , are dealing with is the rule of law. In response to PEGA's question about a possible correlation, the Commission states that it does 'not have enough information at its disposal allowing us to draw definitive conclusions about a link between geolocation and a possible device infection attempt via Pegasus'[285] .***	144. According to the Commission, 'it is impossible to attribute these indicators to a specific perpetrator with full certainty.' The Commission holds that it cannot elaborate on the investigation's present-day findings, as 'they would reveal to adversaries the Commission's investigation methods and capabilities, thus seriously jeopardizing the institution's security'.

[284] https://pro.politico.eu/news/148627

[285] Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022,

Or. en

Amendment 1041
Sophia in 't Veld

Motion for a resolution
Paragraph 145

Motion for a resolution	*Amendment*
145. In its interaction with the PEGA committee, the Commission repeatedly explained that the hack of Commissioner Reynders's device with Pegasus software did not succeed, seemingly downplaying the gravity of a Commissioner being targeted. However, any attempted hack - successful or not - of (a member of) the Commission is a very grave political fact that affects the integrity of the democratic decision-making process.	145. In its interaction with the PEGA committee, the Commission repeatedly explained that the hack of Commissioner Reynders's device with Pegasus software did not succeed, seemingly downplaying the gravity of a Commissioner being targeted. However, any attempted hack - successful or not - of (a member of) the Commission is a very grave political fact that affects the integrity of the democratic decision-making process. ***The fact that the Commission did not wish to comment any further on the attempted hack of Commissioner Reynders's device and the potential hack of Commission staff, neither in in camera sessions of the PEGA committee, is regrettable.***

Or. en

Amendment 1042
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 146

Motion for a resolution	*Amendment*
146. Following the attempted hack of Commissioner Reynders's phone and the indicators of compromise on several devices of Commission staff, the Commission deployed a mobile 'Endpoint Detection and Response' (EDR) solution on all corporate phones in September 2021.	146. Following the attempted hack of Commissioner Reynders's phone and the indicators of compromise on several devices of Commission staff, the Commission deployed a mobile 'Endpoint Detection and Response' (EDR) solution on all corporate phones in September 2021. ***This solution would help the Commission's services to "identify potentially infected corporate mobile devices. Whenever there are indications of infections, a security review of the device***

is organised." The Commission says to cooperate continuously with CERT-EU, the Computer Emergency Response Team of the Union's institutions, bodies, and agencies, and to issue recommendations and guidance to CERT-EU's constituents[285a]. Due to the lack of information the Committee has received from the Commission, it is unclear to what extent the Commission's measures to analyse previous spyware attacks have been successful and to what extent the measures implemented are sufficient in the future.

[285a] Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022

Or. en

Amendment 1043
Sophia in 't Veld

Motion for a resolution
Paragraph 146

Motion for a resolution	*Amendment*
146. Following the attempted hack of Commissioner Reynders's phone and the indicators of compromise on several devices of Commission staff, the Commission deployed a mobile 'Endpoint Detection and Response' (EDR) solution on all corporate phones in September 2021.	146. Following the attempted hack of Commissioner Reynders's phone and the indicators of compromise on several devices of Commission staff, the Commission deployed a mobile 'Endpoint Detection and Response' (EDR) solution on all corporate phones in September 2021. ***This solution would help the Commission's services to "identify potentially infected corporate mobile devices. Whenever there are indications of infections, a security review of the device is organised." The Commission says to cooperate continuously with CERT-EU, the Computer Emergency Response Team of the Union's institutions, bodies, and agencies, and to issue recommendations and guidance to CERT-EU's***

constituents[1a].

[1a] Response letter by Commissioners Hahn and Reynders to the PEGA committee - 9 September 2022

Or. en

Amendment 1044
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Subheading 106

Motion for a resolution	*Amendment*
Targeting of former Greek Commissioner and representatives in the Council	***deleted***

Or. en

Amendment 1045
Vladimír Bilčík, Elissavet Vozemberg-Vrionidi, Juan Ignacio Zoido Álvarez, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 147

Motion for a resolution	*Amendment*
147. On 6 November, Greek newspaper Documento published an extensive list of people who have allegedly been found to have traces of Predator on their devices, including Dimitris Avramopoulos, European Commissioner from 2014-2019 and Néa Dimokratía politician[286] . ***It is not clear whether he was targeted while he was member of the College, and who was behind, but considering the long list of targeted people, including many politicians from both Néa Dimokratía and opposition, the most plausible hypothesis is that the orders came from the***	147. On 6 November, Greek newspaper Documento published an extensive list of people who have allegedly been found to have traces of Predator on their devices, including Dimitris Avramopoulos, European Commissioner from 2014-2019 and Néa Dimokratía politician[286] .

entourage of the Prime Minister.

[286] Documento, edition 6 November 2022.

[286] Documento, edition 6 November 2022.

Or. en

Amendment 1046
Vladimír Bilčík, Elissavet Vozemberg-Vrionidi, Juan Ignacio Zoido Álvarez, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 148

Motion for a resolution	*Amendment*
148. This case therefore demonstrates that (former) Commissioners, including their communications with colleagues, can be targeted for domestic political reasons at any given moment from within their Member States. Moreover, among the list of targets published by Documento, there are several current government ministers, including the ones of Foreign Affairs and Finance. These ministers are also members of the Council, deciding on EU foreign and finance policy. Therefore, a single infected phone could also serve to wiretap in real-time all Commission and Council meetings.	***deleted***

Or. en

Amendment 1047
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 148 a (new)

Motion for a resolution	*Amendment*
	148 a. National security is enshrined in Article 4(2) TEU as a matter of sole

national responsibility. As a provision of primary law, it has a constitutional character and prevails over secondary law which cannot be in contradiction with Article 4 TEU. According to CJEU case law the exclusive responsibility of Member States to provide national security, corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities. Subject to meeting the other requirements laid down in Article 52(1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives. The Court of Justice has also stated that although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, "the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law".

Or. en

Amendment 1048
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 a (new)

Motion for a resolution	*Amendment*
	148 a. Ia (new) Use of spyware in third countries directly or indirectly involving entities linked to the EU

Or. en

Amendment 1049
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 148 b (new)

Motion for a resolution	*Amendment*
	148 b. Several fundamental rights enshrined in the Charter may be affected by the use of spyware. First of all, such use may interfere with the right to privacy, family life and confidentiality of communications (Article 7). It may also interfere with the right to data protection (Article 8) and the right to freedom of expression guaranteed in Article 11, which constitutes one of the essential foundations of a pluralist, democratic society. The right to property (Article 17) could be affected by the placing of spyware on a targets phone. Furthermore, equality before the law (Article 20) and non-discrimination (Article 21) could be affected, and, the right to a fair trial (Article 47) may also be compromised. Spyware can also have chilling effects on other human rights and fundamental freedoms, including the right to dignity (Article 1), freedom of assembly (Article 12), freedom of religion (Article 11), and even the physical and psychological integrity of an individual (Article 3).

Or. en

Amendment 1050

Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 b (new)

Motion for a resolution	*Amendment*
	148 b. The following section will highlight to what extent the use of the Pegasus or equivalent surveillance spyware, directly or indirectly involving entities linked to the EU, contributed to illegal spying on journalists, politicians, law enforcement officials, diplomats, lawyers, business people, civil society actors, human rights defenders or other actors in third countries. This includes, to what extent the deployment of spyware has led to human rights violations that are of serious concern as regards the objectives of the EU's common foreign and security policy, and whether such use was in contravention of the values enshrined in Article 21 TEU and in the Charter, also with due regard to the United Nations Guiding Principles on Business and Human Rights and other rights enshrined in international human rights law.

Or. en

Amendment 1051
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 c (new)

Motion for a resolution	*Amendment*
	148 c. The abuse of spyware technologies by third countries has both direct and indirect impact on the EU, as well as its foreign policy agenda, in particular in its

relation to Israel and Morocco. Moreover, the close cooperation between the EU and both countries can also be observed in the areas of security policy, such as the data exchange agreements currently under negotiation. Among the third countries involved with spyware, both countries have received particular attention from the PEGA Committee, with a hearing and mission to Israel in July 2022, and a session dedicated to Morocco in February 2023 during a hearing on geopolitics of spyware.

Or. en

Amendment 1052
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 148 c (new)

Motion for a resolution	*Amendment*
	148 c. Article 52(1) of the Charter lays down the conditions for the limitation of the exercise of fundamental rights. A limitation must be provided for by law, respect the essence of the rights and freedoms concerned, be subject to the principle of proportionality, and only be imposed if it is necessary (strict necessity) and genuinely meets objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

Or. en

Amendment 1053
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 148 d (new)

Motion for a resolution	*Amendment*
	148 d. All EU countries have legal framework for the use, import, sale, etc. of cyberweapons, including spyware like Pegasus or equivalent. In all cases however, this framework, which applies to the general population, includes specific exceptions for law enforcement and intelligence agencies. Their use is often included under the umbrella of "special investigative techniques", and is regulated by criminal procedural codes, laws on internal security or equivalent measures. In democratic societies, a balance has to be reached between ensuring intelligence and security services can operate effectively, while complying with democratic norms and standards.

Or. en

Amendment 1054
Hannah Neumann, Saskia Bricmont, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja, Diana Riba i Giner
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 d (new)

Motion for a resolution	*Amendment*
	148 d. 1. Israel

Or. en

Amendment 1055
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold, Andrzej Halicki, Bartosz Arłukowicz, Radosław Sikorski

Motion for a resolution
Paragraph 148 e (new)

Motion for a resolution	*Amendment*
	148 e. Venice Commission provided recommendations with respect to democratic accountability of security and intelligence services pursuing surveillance. The rules on the mandate of the security organisations have to be clear and concise and should only be kept secret if absolutely necessary. Internal control of the agency is identified as the main guarantee against abuses of power. This can be influenced by the quality of the staff and its commitment to democratic principles, the existence of an independent official tasked with overseeing the agency and clear internal rules on decision-making processes. Venice Commission's standards with respect to parliamentary accountability focus on autonomy and independence of an oversight body as well as adequate expertise of its members. In terms of judicial accountability, the judges must be independent and should possess the necessary expertise. Finally, the Venice Commission the necessity for the possibility for a victim to seek redress before an independent body.

Or. en

Amendment 1056
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 e (new)

Motion for a resolution	*Amendment*
	148 e. A study commissioned by the European Parliament and published in 2023 under the title Pegasus and the EU's external relations noted that " for exporting countries, the spyware industry can be a lucrative source of revenue and a

lever for diplomatic influence". This is also confirmed by news reports, where experts confirm the usefulness of Pegasus in forging diplomatic relations, ie with Gulf states[1a].

[1a] https://www.france24.com/en/live-news/20210719-pegasus-scandal-shows-risk-of-israel-s-spy-tech-diplomacy-experts

Or. en

Amendment 1057
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 f (new)

Motion for a resolution	*Amendment*
	148 f. Israel's intelligence agency, particularly its cybersecurity division, Unit 8200 is at the heart of Israel's successful spyware industry, as many Israeli firms enjoy close relations with the entity, as the study finds. It further states that "a 2018 study cited in Haaretz found that 80 percent of the 2,300 people who founded Israel's 700 cybersecurity companies were former employees of the Israeli Defense Forces' intelligence units"[1b]. One of its most prominent figures is Intellexa owner and founder Tal Dilian (see Chapter on Intellexa and Tal Dilian).

[1b] Haaretz (2018), Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays, https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-

and-gays/0000017f-e9a9-dc91-a17f-fdadde240000?lts=1664304435322

Or. en

Amendment 1058
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 g (new)

Motion for a resolution	*Amendment*
	148 g. Israeli spyware companies have sold surveillance technology throughout the world including to 14 EU member states as well as to authoritarian Gulf countries. It is believed that the sale of Pegasus facilitated negotiations for establishing formal diplomatic ties under the so called Abraham Accords with Morocco, Bahrain, and formally also the United Araba Emirates[1c]. The industry's collective sales are estimated to be at least $1 billion annually [1d] .
	[1c] Haaretz (2022) Netanyahu Used NSO's Pegasus for Diplomacy, https://www.haaretz.com/israel-news/2022-02-05/ty-article/.premium/netanyahu-used-nsos-pegasus-for-diplomacy-now-he-blames-it-for-his-downfall/0000017f-e941-dc91-a17f-fdcd55c80000
	[1d] Rest of World (2021), Inside Israel's lucrative — and secretive — cybersurveillance industry

Or. en

Amendment 1059
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja

on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 h (new)

Motion for a resolution	*Amendment*
	148 h. Following the US decision to place the NSO Group on its Entity List, the reaction from Israel's government was prompt. Israeli diplomats were said to be orchestrating a diplomatic "campaign" to remove sanctions against NSO as well as Candiru, seeking to "persuade the Biden administration" that the companies' activities remained of "great importance" to the national security of both countries[1e] .
	[1e] The New York Times (2021), Despite Abuses of NSO Spyware, Israel Will Lobby U.S. to Defend It, https://www.nytimes.com/2021/11/08/world/middleeast/nso-israel-palestinians-spyware.html

Or. en

Amendment 1060
Hannah Neumann, Saskia Bricmont, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja, Diana Riba i Giner
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 i (new)

Motion for a resolution	*Amendment*
	148 i. In addition to the diplomatic ties, the use of Pegasus and equivalent spyware within Israel and the occupied Palestinian Territories has an impact on EU's external policy and the development of spyware in Israel cannot be seen in isolation from the country's domestic political and regional political context, which has been characterized as as

"incubator for oppressive technology"[1f].

[1f] France 24 (2021) Pegasus scandal shows risk of Israel's spy-tech diplomacy: experts https://www.france24.com/en/live-news/20210719-pegasus-scandal-shows-risk-of-israel-s-spy-tech-diplomacy-experts

Or. en

Amendment 1061
Hannah Neumann, Saskia Bricmont, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja, Diana Riba i Giner
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 j (new)

Motion for a resolution	*Amendment*
	148 j. Many surveillance technologies, including spyware, have been used in violation of international human rights in Israel, notably on Palestinians and individuals residing in occupied territories. In the latter, Palestineans are disproportionately affected by surveillance systems, such as biometric recognition and spyware. According to credible reports the Israeli military over the last two years has rolled out a broad surveillance effort in the occupied West Bank to monitor Palestinians by integrating facial recognition with a growing network of cameras and smartphones[1g].

[1g] https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html

Or. en

Amendment 1062
Hannah Neumann, Saskia Bricmont, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja, Diana Riba i Giner
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 k (new)

Motion for a resolution	*Amendment*
	148 k. Surveillance technology is in most cases deployed against the consent of those affected and deprives these individuals of their right to privacy, freedom of expression and the right to an open, secure and free Internet [1h1i] According to experts, Israel's readiness to test new surveillance systems on Palestinians in the occupied territories, creates incentives for a business model in the surveillance industry, which also NSO has benefited from, as the company's exports do not amount to a crime under Israeli law[1j]. As a result, countries acquiring "field trained" spyware from Israel contribute to human rights violations in the aforementioned regions. EU Member States, as some of NSO's most prestigious clients, are therefore in direct contradiction of EU foreign and security policy agenda regarding the support of human rights and democracy[1k].

[1h] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on surveillance and human rights https://www.ohchr.org/Documents/Issues/Opinion/A_HRC_41_35_EN.docx

[1i] Answer given by High Representative/Vice-President Borrell on behalf of the European Commission of 21 October 2021 on a written question regarding the blocking and censorship of Pro-Palestinean social media content

[1j] France 24 (2021) Pegasus scandal

shows risk of Israel's spy-tech diplomacy: experts https://www.france24.com/en/live-news/20210719-pegasus-scandal-shows-risk-of-israel-s-spy-tech-diplomacy-experts

[1k] In line with most findings of the 2021 Annual Report on the "Application of the EU Charter of Fundamental Rights 'Protecting Fundamental Rights in the Digital Age", the EU is obliged to facilitate the work of HRDs online.

Or. en

Amendment 1063
Hannah Neumann, Saskia Bricmont, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja, Diana Riba i Giner
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 l (new)

Motion for a resolution	*Amendment*
	148 l. NSO's Pegasus spyware has been used to target Palestinian civil society, among them six Palestinian human rights defenders[1l][1m] . In the cases of Ubai Al-Aboudi, executive director of Bisan Center for Research and Development and Salah Hammouri, a dual French national, lawyer and field researcher at Addameer Prisoner Support and Human Rights Associations, the use of surveillance spyware appears to have resulted in their administrative detention. The surveillance of all six individuals coincides with the highly controversial designation of six Palestinian human rights organisations as "terrorist", sparking an international outcry condemning the decision by the Israeli government. Among the critics, the UN[1n] and human rights organisations who have denounced the surveillance of Palestinian civil society, pointing out the possible "chilling effects" this might have on

freedom of expression and freedom of assembly[1o]. The case of surveillance of Palestinian human rights defenders is yet another proof for lack of enforcement of NSO's Human Rights Policy[1p], which the company has used to boost its legitimacy and credibility when selling to EU Member States.

1l

https://www.frontlinedefenders.org/en/statement-report/statement-targeting-palestinian-hrds-pegasus

1m

https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/

1n ***https://www.ohchr.org/en/press-releases/2021/10/un-experts-condemn-israels-designation-palestinian-human-rights-defenders?LangID=E&NewsID=27702***

1o

https://www.hrw.org/news/2021/11/08/spyware-used-hack-palestinian-rights-defenders

1p

https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/

Or. en

Amendment 1064
Hannah Neumann, Saskia Bricmont, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja, Diana Riba i Giner
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 m (new)

Motion for a resolution	*Amendment*

148 m. Despite these revelations, which have demonstrated rights violations against Palestinian civil society over many years, it appears that multiple EU Member States continue to be clients of NSO. Contrary to the US, the actions of NSO have not led to any notable disruption regarding the EU and its relationship to the Israeli government or any changes with regards to the EU's foreign policy agenda. It shall be noted that the Commission engaged with the Israeli authorities regarding reports of misuse of NSO's Pegasus spyware in violation of human rights. In a letter to the PEGA Committee of 09 September 2022, the Commission replied that it had addressed concerns of potential misuse with the Israeli export authorities and "sought indications on any related mitigating measures that competent Israeli export control authorities could consider taking in the future". At the time of the letter, the Commission had not received any such indications from the competent Israeli export control authorities but intended "to return to the issue of possible mitigating measures at the next meeting of the EU-Israel Subcommittee on Industry, Trade and Services of the Association Agreement".

Or. en

Amendment 1065
Hannah Neumann, Saskia Bricmont, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja, Diana Riba i Giner
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 n (new)

Motion for a resolution	*Amendment*
	148 n. Morocco

Or. en

Amendment 1066
Hannah Neumann, Saskia Bricmont, Gwendoline Delbos-Corfield, Diana Riba i Giner, Marcel Kolaja, Jordi Solé
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 o (new)

Motion for a resolution	*Amendment*
	148 o. Multiple news reports have documented the widespread use of spyware by Morocco. With a licence for about 10.0000 phone numbers, Morocco can be considered as one of NSO's biggest Pegasus clients. In the course of the Pegasus project it was revealed that numbers belonging to European Council President Charles Michel, French president Emmanuel Macron and dozens of French officials, as well as Romano Prodi, a former Italian prime minister, appeared among targeted numbers by Morocco[1a]. In addition, more than 200 numbers in Spain were allegedly spied on by the government, among them prime minister Pedro Sanchez as well as journalists and activists[1b]. Morocco has refuted the accusation tied to the Pegasus Project as "erroneous".

1a
https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/

1b
https://www.npr.org/2022/05/11/1098368201/a-spying-scandal-and-the-fate-of-western-sahara

Or. en

Amendment 1067
Hannah Neumann, Saskia Bricmont, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja, Diana Riba i Giner
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 p (new)

Motion for a resolution	*Amendment*
	148 p. The revelations also demonstrated that within the country, surveillance with spyware has been used to hack and subsequently intimidate journalists and activists[1c]. In a recent resolution on the surveillance and imprisonment of investigative journalist Omar Radi, the European Parliament has condemned the Moroccan government's sustained judicial harassment against journalists and urged the country "to end their surveillance of journalists, including via NSO's Pegasus spyware"[1d]. One of the targeted individuals, Ignacio Cembrero, an investigative journalist at the Spanish newspaper El Confidential, appeared before the Committee on 29 November. He was made aware of the hacking of his phone after text messages between him and the Spanish government were published in a Moroccan newspaper. Upon the request of a Spanish court to cooperate, Israeli authorities have refused to supply further information to aid the case.

[1c] https://daraj.media/en/76202/

[1d] European Parliament resolution of 19 January 2023 on the situation of journalists in Morocco, notably the case of Omar Radi (2023/2506(RSP)) https://www.europarl.europa.eu/doceo/document/TA-9-2023-0014_EN.html

Or. en

Amendment 1068
Hannah Neumann, Saskia Bricmont, Gwendoline Delbos-Corfield, Diana Riba i Giner, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 q (new)

Motion for a resolution	*Amendment*
	148 q. Morocco also persecuted Moroccan journalists in French exile Hicham Mansouri and Aboubakr Jamaim[1e] as well as supporters of the Western Sahara, namely Paris-based defence lawyer Joseph Breham and Belgium-based Sahrawi Human rights defender El Mahjoub Maliha[1f].
	[1e] Forbidden Stories. https://forbiddenstories.org/journaliste/hicham-mansouri/, https://forbiddenstories.org/journaliste/aboubakr-jamai/
	[1f] https://www.middleeasteye.net/fr/entretiens/pegasus-espionnage-maroc-france-macron-sahara-occidental-breham-avocat-mangin-algerie

Or. en

Amendment 1069
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 r (new)

Motion for a resolution	*Amendment*
	148 r. Morocco has launched several legal proceedings against accusations of its involvement in the use of Pegasus in France, Spain, and Germany. In France, the Moroccan authorities filed defamation suits against several media outlets and civil society organisations, including Le Monde, Forbidden Stories, Radio France, Mediapart, L'Humanité and Amnesty International. On 25 March 2022, the

Paris Correctional Court dismissed the cases as inadmissible and the Moroccan authorities appealed the decision. In Spain, the Moroccan authorities filed a case against journalist Cembrero on a Medieval Age-old clause in the Penal Code of "an act of bragging". The case is ongoing and has been denounced as seeking to intimidate Cembrero and others from reporting on Morocco's use of the spyware.

Or. en

Amendment 1070
Hannah Neumann, Saskia Bricmont, Gwendoline Delbos-Corfield, Diana Riba i Giner, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 s (new)

Motion for a resolution	*Amendment*
	148 s. According to a news report, prior to its widespread use of Pegasus, Morocco was also client of at least three European spyware providers, the French companies Amesys and Vupen[1f], as well as the Italian Hacking Team. According to confidential documents, Morocco was the third largest client of the Italian company and paid more than 3 million euros over six years to acquire Hacking Team's RCS software for its domestic High Council for National Defence (CSDN) and the Directory of Territorial Surveillance (DST)[1g]. With the help of the spyware, multiple high level UN departments and services have been surveilled.

1f
https://moroccomail.fr/2022/09/21/morocco-used-hacking-team-to-spy-on-the-un/

1g
https://privacyinternational.org/blog/1394/facing-truth-hacking-team-leak-

confirms-moroccan-government-use-spyware

Or. en

Amendment 1071
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 t (new)

Motion for a resolution	*Amendment*
	148 t. Morocco has not only acquired spyware in the EU but has also been supplied with technological and financial support by the European Commission. According to a report, Morocco received two spyware systems to spy on individuals for border control purposes (French-Lebanese MSAB's spyware "XRY" and US-based Oxygen Forensics spyware called "Detective"[1h]). In addition, the European Union Agency for Law Enforcement Training (CEPOL) was sent to Morocco to conduct in-person training on how to use spyware and also teach the police how to extract information from social media profiles via social hacking[1i]. Contrary to Pegasus, the spywares mentioned can only enter the device physically and do not leave any traces of its use. The report outlines multiple cases, among them journalists and activists, in which smartphones have been taken away from targets and returned with hints towards possible infiltration afterwards. Despite the fact that there is no possibility to verify whether the spyware has been used properly by third parties (as the spyware does not leave any traces), there were no indications that the Commission verified the proper use of the supplied technologies. Similar to a complaint to the EU Ombudsman on the funding for

surveillance technologies under the EUTFA programme (see chapter below), no impact assessment have been conducted by the Commission to map possibly misuse of the supplied technologies.The Commission has stated that it is up to the user, Morocco, to deploy the spyware responsibly and according to the contractual agreement (for outlined purposes only)[1j].

[1h]

https://www.spiegel.de/ausland/marokko-wie-die-eu-rabats-ueberwachungsapparat-aufruestet-a-d3f4c00e-4d39-41ba-be6c-e4f4ba650351

[1i] ***https://privacyinternational.org/long-read/4289/revealed-eu-training-regime-teaching-neighbours-how-spy***

[1j] ***https://disclose.ngo/en/article/how-the-eu-supplied-morocco-with-phone-hacking-spyware***

Or. en

Amendment 1072
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 u (new)

Motion for a resolution	*Amendment*
	148 u. 3. Other third countries

Or. en

Amendment 1073
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 v (new)

Motion for a resolution	*Amendment*
	148 v. Globally, at least 75 countries have purchased and/or used spyware, including repressive regimes[1a]. Human rights organizations have documented numerous incidents where spyware has been misused to target politicians, journalists, lawyers, human rights defenders and other civil society activists promoting human rights, women's rights, and environmental protection[1b].
	[1a] Carnegie Endowment for International Peace (11 January 2023): Global Inventory of Commercial Spyware & Digital Forensics https://carnegieendowment.org/programs/democracy/commercialspyware
	[1b] Forensic Architecture/ Amnesty International / The Citizenlab: Digital Violence https://www.digitalviolence.org/#/

Or. en

Amendment 1074
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 w (new)

Motion for a resolution	*Amendment*
	148 w. In a number of cases, authorities specifically target women activists with spyware, in order to extract information for defamation campaigns. Due to the increased social scrutiny women are under, public shaming of women by leaking private and intimate information may particularly trigger harassment,

social ostracism and even physical attacks[1c].

---

*[1c] **Frontline Defenders (2021): Unsafe anywhere: women human rights defenders speak out about Pegasus attacks https://www.frontlinedefenders.org/sites/default/files/unsafe-anywhere_-women-human-rights-defenders-speak-out-about-pegasus-attacks_en.pdf***

Or. en

Amendment 1075
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 x (new)

Motion for a resolution	*Amendment*
	148 x. 3.1. Spyware produced by EU-based companies exported to third countries

Or. en

Amendment 1076
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 y (new)

Motion for a resolution	*Amendment*
	148 y. Several types of spyware produced by EU-based companies have been exported to third countries, including those where cases of abuse have been documented. Greece-based Intellexa

company's spyware product Predator was found in Armenia, Egypt, Greece, Indonesia, Madagascar, Oman, Saudi Arabia, and Serbia. According to a CitizenLab report in June 2021, two Egyptians, including exiled politician Ayman, were hacked with Predator spyware[1d]. Another country with a poor human rights record that has received Predator is Sudan, as recently reported[1e].

[1d] CitizenLab: Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware. https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

[1e] Lighthouse Reports, Flight of the Predator https://www.lighthousereports.nl/investigation/flight-of-the-predator/

Or. en

Amendment 1077
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 z (new)

Motion for a resolution	*Amendment*
	148 z. The Germany-based, now dissolved, company FinFisher, produced the spyware FinSpy which has been used in at least 32 countries, including numerous with a poor human rights record, like Angola, Bahrain, Bangladesh, Egypt, Ethiopia, Gabon, Jordan, Kazakhstan, Lebanon, Morocco, Myanmar, Nigeria, Oman, Qatar, Saudi Arabia, Turkey and Turkmenistan[1f]. In a number of third countries the abusive targeting of critical voices with FinSpy

has been documented: In 2011, Ahmed Mansoor, a human rights defender in the United Arab Emirates, was targeted with FinFisher's FinSpy spyware[1g]. FinFisher helped Bahrain install spyware on 77 computers, including those belonging to human rights lawyers[1h]. In 2012, FinFisher's software enabled the surveillance of Ethiopian political refugee Tadesse Kersmo by the Ethiopian government after he fled into EU exile[1i].

[1f] The Citizenlab (15 Oktober 2015) Pay No Attention to the Server Behind the Proxy, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

[1g] CitizenLab: The Million Dollar Dissident. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

[1h] Amnesty International: A brief history of governments hacking human rights organizations. https://www.amnesty.org/en/latest/campaigns/2016/01/brief-history-of-government-hacking-human-rights-organizations/

[1i] Privacy International:Surveillance follows Ethiopian political refugee to the UK. https://privacyinternational.org/blog/1199/surveillance-follows-ethiopian-political-refugee-uk

Or. en

Amendment 1078
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 aa (new)

Motion for a resolution	*Amendment*
	148 aa. Since 2012 Italy-based company Hacking Team, now Memento Lab, sold its spyware RCS to numerous authoritarian countries, including Ethiopia, Bahrain, Egypt, Kazakhstan, Morocco, Russia, Saudi Arabia, Sudan, Azerbaijan and Turkey. An inquiry launched by NGOs as well as UN investigators into the export of RCS presence to Sudan eventually led the Italian authorities to impose stricter export rules for the company[1j].
	1j https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/ https://netzpolitik.org/2022/pega-untersuchungsausschuss-wie-staatstrojaner-gegen-eu-buerger-eingesetzt-werden/

Or. en

Amendment 1079
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 ab (new)

Motion for a resolution	*Amendment*
	148 ab. The French surveillance company Amesys has supplied the former Libyan regime of Moamar al-Gaddafi with a sophisticated electronic surveillance system, which helped identify Libyan human rights defenders (HRDs), and led to their arrest and then torture. At least five Libyan HRDs were arrested and tortured after their online communications were intercepted by Amesys' system[1k].

[1k] ***https://www.fidh.org/en/region/north-africa-middle-east/egypt/sale-of-surveillance-equipment-to-egypt-by-french-company-amesys***

Or. en

Amendment 1080
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 ac (new)

Motion for a resolution	*Amendment*
	148 ac. On November 21, 2022, the Investigative Chamber of the Paris Court of Appeal confirmed the indictment of Amesys and its executives for complicity in acts of torture committed in Libya and ordered the continuation of the investigation[1l]. In 2017, it was revealed that Amesys sold a similar system to the Egyptian regime after it had changed its name and following the European Council's decision on 21 August 2013 "to suspend export licenses to Egypt for any equipment that could be used for domestic repression". Three civil society organizations —FIDH and the Ligue des Droits de l'Homme (France), and the Cairo Institute for Human Rights Studies— filed a criminal complaint in France relating to the potential role of Amesys in the forced disappearance, detention, and torture of political activists and dissidents since 2013[1m].

[1l] ***https://www.fidh.org/en/impacts/Surveillance-torture-Libya-Paris-Court-Appeal-indictment-AMESYS***

[1m] ***https://www.telerama.fr/monde/amesys-***

egyptian-trials-and-tribulations-of-a-french-digital-arms-dealer,160452.php

Or. en

Amendment 1081
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 ad (new)

Motion for a resolution	*Amendment*
	148 ad. In 2014, French company Ercom sold two surveillance systems to the Egyptian authorities. A communications interception tool called Vortex and another data processing tool named Cortex. Both allow the Egyptian government to intercept calls and SMS, monitor internet traffic, and identify the geo-location of a target[1n].
	1n
	https://www.fidh.org/en/issues/litigation/egypt-a-repression-made-in-france

Or. en

Amendment 1082
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 ae (new)

Motion for a resolution	*Amendment*
	148 ae.3.2. EU member states' complicity as NSO group clients for Pegasus abuse in third countries

Or. en

Amendment 1083
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 af (new)

Motion for a resolution	*Amendment*
	148 af. At least 14 EU Member States have purchased the Pegasus spyware of the NSO group and have thus become complicit of the company's facilitation of human rights violations outside the EU They legitimize the business model of the company and provide it with financial means that can be used to improve its products that are also sold to repressive regimes to commit human rights violations.

Or. en

Amendment 1084
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 ag (new)

Motion for a resolution	*Amendment*
	148 ag. The following 14 non-EU country authorities are most likely responsible for more than 150 such cases where victims have been identified and where the infection was technically proven : 31 cases from El Salvador, 29 from Mexico, 25 from Thailand, 14 from Morocco, 13 from India, 9 from Rwanda, 9 from Saudi Arabia, 5 from Bahrain, 4 from Jordan, 4 from Kazakhstan, 4 from

Togo, 4, from the UAE, 3 from Israel, 2 from Azerbaijan[1o].

[1o] https://spywarefiles.eu/

Or. en

Amendment 1085
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 ah (new)

Motion for a resolution	*Amendment*
	148 ah. The so-called Pegasus Project, a collaboration by more than 80 journalists from 17 media has documented how Pegasus has been used by repressive governments seeking to silence journalists, attack activists and crush dissent. Investigations by the Pegasus Project have shown that family members of Saudi journalist Jamal Khashoggi were targeted with Pegasus software before and after his murder in Istanbul on 2 October 2018 by Saudi operatives, despite repeated denials from NSO Group. Amnesty International's Security Lab established that Pegasus spyware was successfully installed on the phone of Khashoggi's fiancée Hatice Cengiz just four days after his murder. His wife, Hanan Elatr was also repeatedly targeted with the spyware between September 2017 and April 2018 as well as his son, Abdullah, who was also selected as a target along with other family members in Saudi Arabia and the UAE[1p].

[1p] Amnesty International (19 July 2021) Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally,

https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

Or. en

Amendment 1086
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 ai (new)

Motion for a resolution	*Amendment*
	148 ai. Investigations by the Pegasus-Project have documented that journalists have been frequent targets of the Pegasus spyware: In Mexico, journalist Cecilio Pineda's phone was selected for targeting just weeks before his killing in 2017. Pegasus has been used in Azerbaijan, a country where only a few independent media outlets remain. More than 40 Azerbaijani journalists were selected as potential targets according to the investigation. Amnesty International's Security Lab found the phone of Sevinc Vaqifqizi, a freelance journalist for independent media outlet Meydan TV, was infected over a two-year period until May 2021. In India, at least 40 journalists from nearly every major media outlet in the country were selected as potential targets between 2017-2021. Forensic tests revealed the phones of Siddharth Varadarajan and MK Venu, co-founders of independent online outlet The Wire, were infected with Pegasus spyware as recently as June 2021[1q].

[1q] Amnesty International (19 July 2021) Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally, https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

Or. en

Amendment 1087
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 148 aj (new)

Motion for a resolution	*Amendment*
	148 aj. Human rights defenders continue to be frequently targeted, including by the authorities of the following countries: Mexico, El Salvador, Morocco, Rwanda, Israel, Jordan, Saudi Arabia, Bahrain, United Arab Emirates, India and Kazakhstan[1r]. In 2021 Frontline Defenders published a report documenting the targeted surveillance of human rights defenders including in India. In June 2018 sixteen human rights defenders were jailed under anti-terror law, in what is known as the Bhima Koregaon case, which relates to the violence that took place in Bhima Koregaon. One of the defenders, 84 year old Jesuit priest, Stan Swamy, died in custody in July 2021[1s]. A digital forensics investigation found that 'evidence' relied on by the prosecution against the group had been planted through Pegasus spyware onto IT devices of human rights defenders Rona Wilson and Surendra Gadling and that there was no evidence that the defenders interacted[1t].
	[1r] https://spywarefiles.eu/
	[1s] Frontline Defenders (2 December 2021): Action needed to address targeted surveillance of human rights defenders https://www.frontlinedefenders.org/en/statement-report/action-needed-address-targeted-surveillance-human-rights-defenders

[It] The Wire (17 December 221) Rona Wilson's iPhone Infected With Pegasus Spyware, Says New Forensic Report, https://thewire.in/rights/rona-wilson-pegasus-iphone-arsenal

Or. en

Amendment 1088
Lukas Mandl

Motion for a resolution
Paragraph 149

Motion for a resolution	*Amendment*
149. The European Union is an attractive place for the trade in surveillance technologies and services, including spyware tools. On the one hand, there are the Member State governments as potential customers. On the other hand, the notion of being 'EU-regulated' serves as a quality label, useful for the global market. The EU internal market offers freedom of movement and beneficial national tax regimes. Procurement rules can be avoided with reference to national security, and governments may use proxies or middlemen, so that the purchase of spyware by public authorities is very hard to detect and prove. The EU has strict export rules, but they can be easily circumvented as Member States seek to get a competitive advantage with deliberate lax national implementation, and enforcement by the European Commission is weak and superficial. ***Indeed, each time the regime for export licenses was tightened in Israel***, several companies ***moved*** their export departments to Europe, ***in particular*** Cyprus[287] [288] . Moreover, several personalities from the spyware industry have obtained EU citizenship in order to be able to operate freely within and from the EU.	149. The European Union is an attractive place for the trade in surveillance technologies and services, including spyware tools. On the one hand, there are the Member State governments as potential customers. On the other hand, the notion of being 'EU-regulated' serves as a quality label, useful for the global market. The EU internal market offers freedom of movement and beneficial national tax regimes. Procurement rules can be avoided with reference to national security, and governments may use proxies or middlemen, so that the purchase of spyware by public authorities is very hard to detect and prove. The EU has strict export rules, but they can be easily circumvented as Member States seek to get a competitive advantage with deliberate lax national implementation, and enforcement by the European Commission is weak and superficial. ***In recent years***, ***there has been a clear trend of*** several ***cyber-security*** companies ***moving*** their export departments to Europe, ***especially*** Cyprus. Moreover, several personalities from the spyware industry have obtained EU citizenship in order to be able to operate freely within and from the EU.

[287] Makarios Drousiotis. State Mafia. Chapter 6. Published 2022.

[288] Haaretz. Cyprus, Cyberspies and the Dark Side of Israeli Intel.

Or. en

Amendment 1089
Christine Anderson, Mathilde Androuët, Gilles Lebreton

Motion for a resolution
Paragraph 149

Motion for a resolution	*Amendment*
149. The European Union is an attractive place for the trade in surveillance technologies and services, including spyware tools. On the one hand, there are the Member State governments as potential customers. On the other hand, the notion of being 'EU-regulated' serves as a quality label, useful for the global market. The EU internal market offers freedom of movement and beneficial national tax regimes. Procurement rules can be avoided with reference to national security, and governments may use proxies or middlemen, so that the purchase of spyware by public authorities is very hard to detect and prove. The EU has strict export rules, but they can be easily circumvented as Member States seek to get a competitive advantage with ***deliberate lax*** national implementation, and enforcement by the European Commission is weak and superficial. Indeed, each time the regime for export licenses was tightened in Israel, several companies moved their export departments to Europe, in particular Cyprus[287][288]. Moreover, several personalities from the spyware industry have obtained EU citizenship in order to be able to operate freely within and from the EU.	149. The European Union is an attractive place for the trade in surveillance technologies and services, including spyware tools. On the one hand, there are the Member State governments as potential customers. On the other hand, the notion of being 'EU-regulated' serves as a quality label, useful for the global market. The EU internal market offers freedom of movement and beneficial national tax regimes. Procurement rules can be avoided with reference to national security, and governments may use proxies or middlemen, so that the purchase of spyware by public authorities is very hard to detect and prove. The EU has strict export rules, but they can be easily circumvented as Member States seek to get a competitive advantage with ***visibly inadequate*** national implementation, and enforcement by the European Commission is weak and superficial. Indeed, each time the regime for export licenses was tightened in Israel, several companies moved their export departments to Europe, in particular Cyprus[287][288] Moreover, several personalities from the spyware industry have obtained EU citizenship in order to be able to operate freely within and from the EU.
[287] Makarios Drousiotis. State Mafia.	[287] Makarios Drousiotis. State Mafia.

Chapter 6. Published 2022.	Chapter 6. Published 2022.
[288] Haaretz. Cyprus, Cyberspies and the Dark Side of Israeli Intel.	[288] Haaretz. Cyprus, Cyberspies and the Dark Side of Israeli Intel.

Or. fr

Amendment 1090
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 149 a (new)

Motion for a resolution	*Amendment*
	149 a. Further, as head of Amnesty Tech Claudio Guarniery testified before the PEGA committee, it was European companies like the German FinFisher and the Italian Hacking Team that pioneered the mercenary spyware industry. First reports on the roles of these companies in monitoring journalists and crushing dissent became known over ten years ago when with the advent of protest movements known as the Arab Spring contracts of these companies started emerging from offices of secret police[288a].
	[288a] PEGA Hearing of 30.08.22 on impact of spyware on EU Citizens https://netzpolitik.org/2022/pega-untersuchungsausschuss-wie-staatstrojaner-gegen-eu-buerger-eingesetzt-werden/

Or. en

Amendment 1091
Sophia in 't Veld

Motion for a resolution
Paragraph 149 a (new)

Motion for a resolution	*Amendment*
	149 a. The spyware industry has a spaghetti-like structure: complex, opaque and elusive. Whoever tries to map out the sector will get lost in an impenetrable maze of persons, locations, connections, ownership structures, letterbox companies, ever changing corporate names, money flows, government proxies and middlemen, tycoons and governments. This seems to be a strategy of deliberate "corporate obfuscation".

Or. en

Amendment 1092
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 149 b (new)

Motion for a resolution	*Amendment*
	149 b. The spyware industry has a spaghetti-like structure: complex, opaque and elusive. Whoever tries to map out the sector will get lost in an impenetrable maze of persons, locations, connections, ownership structures, letterbox companies, ever changing corporate names, money flows, government proxies and middlemen, tycoons and governments. This seems to be a strategy of deliberate "corporate obfuscation".

Or. en

Amendment 1093
Gilles Lebreton, Christine Anderson, Mathilde Androuët

Motion for a resolution
Paragraph 150

Motion for a resolution	*Amendment*
150. In many cases, the nickname ‘mercenary spyware’ seems to be accurate. The sector does not have very high ethical standards, selling to the bloodiest dictatorships and wealthy non-state actors with unfriendly intentions. The list of victims of spyware tells the real story, not the hollow human rights pledges in the brochures of the vendors. Even after the Pegasus Project revelations: in 2021 Cellebrite announced it would stop selling to Russia, when it became known that its spyware had been used on anti-Putin activists. However, in October 2022 there are signs that Cellebrite is still being used by Putin[289]. It is a lucrative, booming and shady market***, attracting a lot of cowboys. Still, they get to sell their products to democratic governments in the US and the EU, which grants a veneer of respectability. Nonetheless, despite the claims that the use of spyware is entirely legitimate and necessary, governments are remarkably shy when it comes to admitting they possess spyware. They sometimes resort to the use of proxies, middlemen or brokers for the purchase of spyware, so as to leave no traces***. The big annual event for the industry is the ‘ISS World’ fair, also dubbed ‘The Wiretappers’ Ball’. The home of the annual European edition is Prague. There is considerable overlap between the exhibitors at ISS World and fairs of the arms industry.	150. In many cases, the nickname ‘mercenary spyware’ seems to be accurate. The sector does not have very high ethical standards, selling to the bloodiest dictatorships and wealthy non-state actors with unfriendly intentions. The list of victims of spyware tells the real story, not the hollow human rights pledges in the brochures of the vendors. Even after the Pegasus Project revelations: in 2021 Cellebrite announced it would stop selling to Russia, when it became known that its spyware had been used on anti-Putin activists. However, in October 2022 there are signs that Cellebrite is still being used by Putin[289]. It is a lucrative, booming and shady market. The big annual event for the industry is the ‘ISS World’ fair, also dubbed ‘The Wiretappers’ Ball’. The home of the annual European edition is Prague. There is considerable overlap between the exhibitors at ISS World and fairs of the arms industry.
[289] https://www.haaretz.com/israel-news/security-aviation/2022-10-21/ty-article/.premium/russia-still-using-israeli-tech-to-hack-detainees-cellphones/00000183-eb6c-d15c-a5eb-ff6cf86e0000	[289] https://www.haaretz.com/israel-news/security-aviation/2022-10-21/ty-article/.premium/russia-still-using-israeli-tech-to-hack-detainees-cellphones/00000183-eb6c-d15c-a5eb-ff6cf86e0000
	Or. fr

Amendment 1094
Sophia in 't Veld

Motion for a resolution
Paragraph 150 a (new)

Motion for a resolution	*Amendment*
	150 a. Next to the "official channels" there is also a black market for these products. Although many vendors claim they only sell to governments, it would seem they secretly also try to do business with non-state actors. It is very difficult to find waterproof evidence, as by definition this trade shuns daylight and leaves no traces. Greek newspaper Documento claims to have evidence that the software is being sold on the black market – for up to $50 million – not only to governments and counter-terrorism agencies, but also to private individuals[1a]. Another Greek newspaper, To Vima, reported that Predator was sold to 34 customers from Greece[1b]. Given that spyware is illegal in Greece, that is a stunning number. Leaked documents show a pirated version of the product that was officially sold only to governments, at a price of $8 million, an amount that included training the agents who will use the program, 24-hour technical support and monitoring of the victim's social media accounts[1c].

[1a] Documento. Documento's 'Predator' revelations on Euractiv – Europol's intervention calls for Dutch MEP

[1b] To Vima. Interceptions "Spy software has 34 customers."

[1c] https://en.secnews.gr/417192/ipoklopes-agora-predator-spyware/

Or. en

Amendment 1095
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield,

Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 150 a (new)

Motion for a resolution	*Amendment*
	150 a. Commercial spyware has significantly expanded repressive regimes' capacity to monitor and harass dissidents in exile by compromising even their encrypted communications. As exiles frequently use digital technologies to communicate with contacts at home and to raise awareness about rights violations, spyware enables governments to control, silence, and punish dissent across borders, including through disinformation campaigns or coercion against relatives and others still in the home country[289a].
	[289a] Michaelsen, M.,' The Digital Transnational Repression Toolkit, and Its Silencing Effects', Freedom House, 2020. Available at: https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects

Or. en

Amendment 1096
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 150 b (new)

Motion for a resolution	*Amendment*
	150 b. Next to the "official channels" there is also a black market for these products. Although many vendors claim they only sell to governments, it would

seem they secretly also try to do business with non-state actors. It is very difficult to find waterproof evidence, as by definition this trade shuns daylight and leaves no traces. Greek newspaper Documento claims to have evidence that the software is being sold on the black market – for up to $50 million – not only to governments and counter-terrorism agencies, but also to private individuals. Another Greek newspaper, To Vima, reported that Predator was sold to 34 customers from Greece. Given that spyware is illegal in Greece, that is a stunning number. Leaked documents show a pirated version of the product that was officially sold only to governments, at a price of $8 million, an amount that included training the agents who will use the program, 24-hour technical support and monitoring of the victim's social media accounts.

Or. en

Amendment 1097
Sophia in 't Veld

Motion for a resolution
Paragraph 150 b (new)

Motion for a resolution	*Amendment*
	150 b. The industry offers a wide range of surveillance and intelligence products and services, not just spyware as a single product. Spyware is just one tool in the toolkit of hack-for-hire firms.

Or. en

Amendment 1098
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 150 c (new)

Motion for a resolution	*Amendment*
	150 c. In 2014/15, the Italian spyware company Hacking Team sold spyware to regional governments in Mexico through a private broker who was later convicted of conspiring to sell and use hacking tools and who knew that the equipment sold to Hacking Team's Mexican clients could and likely would be used for political purposes[289c].
	[289c] US Attorneys Office, 15 Feburary 2022 https://www.justice.gov/usao-sdca/pr/mexican-businessman-admits-brokering-spyware-used-monitor-political-and-business-rivals and San Diego Union Tribune, 15 February 2022 https://www.sandiegouniontribune.com/news/courts/story/2022-02-15/elite-hacking-team-mexico-spyware

Or. en

Amendment 1099
Hannah Neumann, Saskia Bricmont, Gwendoline Delbos-Corfield, Diana Riba i Giner, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 150 d (new)

Motion for a resolution	*Amendment*
	150 d. The industry offers a wide range of surveillance and intelligence products and services, not just spyware as a single product. Spyware is just one tool in the toolkit of hack-for-hire firms.

Or. en

Amendment 1100

Ivo Hristov

Motion for a resolution
Paragraph 151

Motion for a resolution	*Amendment*
151. Without vulnerabilities in software, it would be impossible to install and deploy spyware. Therefore, in order to regulate the use of spyware, the discovery, sharing and exploitation of vulnerabilities have to be regulated as well[290] . Despite the strengthening of the defence of digital systems required and encouraged by the NIS2 Directive and the proposal for the Cyber Resilience Act, it is nearly impossible to develop systems without vulnerabilities.	151. Without vulnerabilities in software, it would be impossible to install and deploy spyware. Therefore, in order to regulate the use of spyware, the discovery, sharing and exploitation of vulnerabilities have to be regulated as well[290] . Despite the strengthening of the defence of digital systems required and encouraged by the NIS2 Directive and the proposal for the Cyber Resilience Act, it is nearly impossible to develop systems without vulnerabilities. ***EU may however regulate the handling of vulnerabilities when it comes to the disclosure of information security research with a view of ending the practice of researchers to keep vulnerabilities secret and to sell them to private companies.***
[290] Ot van Daalen, intervention in PEGA 27 October 2022; EDRi Paper: Breaking encryption will doom our freedoms and rightshttps://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-Encryption.pdfhttps://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu	[290] Ot van Daalen, intervention in PEGA 27 October 2022; EDRi Paper: Breaking encryption will doom our freedoms and rightshttps://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-Encryption.pdfhttps://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu

Or. en

Amendment 1101
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 151 a (new)

Motion for a resolution	*Amendment*
	151 a. Vulnerabilities therefore need to be disclosed and fixed as soon as possible. However, current EU law encourages the opposite of disclosure. In the Cybercrime Directive and the Copyright Directive, information security researchers may face civil and criminal liability when doing research into vulnerabilities and sharing their results. Moreover, it is not obligatory for researchers to share any findings on vulnerabilities. Researchers could therefore opt for selling the knowledge of the vulnerability to a private broker, in return for high remunerations.

Or. en

Amendment 1102
Sophia in 't Veld

Motion for a resolution
Paragraph 151 a (new)

Motion for a resolution	*Amendment*
	151 a. Vulnerabilities therefore need to be disclosed and fixed as soon as possible. However, current EU law encourages the opposite of disclosure. In the Cybercrime Directive and the Copyright Directive, information security researchers may face civil and criminal liability when doing research into vulnerabilities and sharing their results. Moreover, it is not obligatory for researchers to share any findings on vulnerabilities. Researchers could therefore opt for selling the knowledge of the vulnerability to a private broker, in return for high remunerations.

Or. en

Amendment 1103
Sophia in 't Veld

Motion for a resolution
Paragraph 151 b (new)

Motion for a resolution	*Amendment*
	151 b. This practice has generated a lively and lucrative trade in vulnerabilities. However, it is not just brokers in zero-days vulnerabilities looking for vulnerabilities: security and law enforcement authorities stockpile vulnerabilities as well, sometimes found by their own experts, sometimes acquired from brokers. If vulnerabilities go unreported, they are not patched, thus leaving our IT systems weakened and the users unprotected. This allows the use of spyware to continue.

Or. en

Amendment 1104
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 151 b (new)

Motion for a resolution	*Amendment*
	151 b. This practice has generated a lively and lucrative trade in vulnerabilities. However, it is not just brokers in zero-days vulnerabilities looking for vulnerabilities: security and law enforcement authorities stockpile vulnerabilities as well, sometimes found by their own experts, sometimes acquired from brokers. If vulnerabilities go unreported, they are not patched, thus leaving our IT systems weakened and the users unprotected. This allows the use of spyware to continue.

Or. en

Amendment 1105
Sophia in 't Veld

Motion for a resolution
Paragraph 152 a (new)

Motion for a resolution	*Amendment*
	152 a. The risk of abuse by the telecom providers of access to these networks is high. We have several documented misuses, where access points (global titles) were leased to shady companies that were monitoring and intercepting communications of targets based on the man-in-the-middle attacks. They were also harvesting geo-location data, meta-data for their own economical purposes. A global title is an address used for routing messages within Signaling System Number 7 (SS7). It can be compared to an IP address, in that the global title refers to an address within the telecommunications system[1a]. This is also the reason why the access to the SS7 network in US was so interesting for NSO, that they were trying to buy their access with "bags of cash"[1b]. Telecom providers are deliberately keeping these low industry standards in order to provide an easier access to local state enforcement agencies.

[1a] https://www.gms-worldwide.com/glossary/global-title/

[1b] https://www.theguardian.com/news/2022/feb/01/nso-offered-us-mobile-security-firm-bags-of-cash-whistleblower-claims

Or. en

Amendment 1106
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 152 a (new)

Motion for a resolution	*Amendment*
	152 a. The risk of abuse by the telecom providers of access to these networks is high. We have several documented misuses, where access points (global titles) where leased to shady companies that were monitoring and intercepting communications of targets based on the man in the middle attacks. They were also harvesting geo-location data, meta-data for their own economical purposes. A global title is an address used for routing messages within Signaling System Number 7 (SS7). It can be compared to an IP address, in that the global title refers to an address within the telecommunications system. This is also the reason why the access to the SS7 network in US was so interesting for NSO, that they were trying to buy their access with "bags of cash".Telecom providers are deliberately keeping these low industry standards in order to provide an easier access to local state enforcement agencies.

Or. en

Amendment 1107
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 152 b (new)

Motion for a resolution	*Amendment*
	152 b. The remainder of this chapter outlines the most prominent actors of the spyware industry in Europe: NSO Group, Intellexa Alliance, Candiru, Tykelab and RCS Lab, DSIRF, and the former FinFisher.

Or. en

Amendment 1108
Sophia in 't Veld

Motion for a resolution
Paragraph 153 a (new)

Motion for a resolution	*Amendment*
	153 a. Since its launch in 2010, NSO Group has had corporate presence in Israel, the UK, Luxembourg, the Cayman Islands, Cyprus, the US, the Netherlands, Bulgaria and the British Virgin Islands. A lot of information regarding the roles of the different corporate entities is still lacking and some of these companies have already been liquidated. NSO Group has however stated in their Transparency and Responsibility report of 2021 that Bulgaria and Cyprus are both export hubs[1a]. According to Amnesty International, the Dutch entities (liquidated on December 22, 2016) functioned in the sector of financial holdings and Q Cyber Technologies as based in Luxembourg was active as a commercial distributor responsible for the issuance of invoices, signing of contracts and receiving payments from customers. In addition, Westbridge Technologies as registered in the US may have facilitated the company's US sales[1b].

[1a] NSO Group. Transparency and Responsibility Report 2021.

[1b] Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.

Or. en

Amendment 1109
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield,

Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 153 a (new)

Motion for a resolution	*Amendment*
	153 a. Since its launch in 2010, NSO Group has had corporate presence in Israel, the UK, Luxembourg, the Cayman Islands, Cyprus, the US, the Netherlands, Bulgaria and the British Virgin Islands. A lot of information regarding the roles of the different corporate entities is still lacking and some of these companies have already been liquidated. NSO Group has however stated in their Transparency and Responsibility report of 2021 that Bulgaria and Cyprus are both export hubs. According to Amnesty International, the Dutch entities (liquidated on December 22, 2016) functioned in the sector of financial holdings and Q Cyber Technologies as based in Luxembourg was active as a commercial distributor responsible for the issuance of invoices, signing of contracts and receiving payments from customers. In addition, Westbridge Technologies as registered in the US may have facilitated the company's US sales.

Or. en

Amendment 1110
Sophia in 't Veld

Motion for a resolution
Paragraph 153 b (new)

Motion for a resolution	*Amendment*
	153 b. NSO reportedly had revenues of $243 million in 2020[1a]. However, following the revelations by the Pegasus Project, the company faced several difficulties. Lawsuits filed by Apple[1b] and

Meta[1c] against the company, blacklisting of NSO by the US Commerce department, the tightening of the Israeli export regime, critical inquiries in several countries, and internal frictions within the private equity fund behind NSO group, have led to a severe decline in profit. Reportedly, NSO Group's debt at one point even reached 6.5 times its normal revenues for a year[1d].

[1a] Haaretz. NSO Is Having a Bad Year - and It's Showing.

[1b] Apple. Apple sues NSO Group to curb the abuse of state-sponsored spyware.

[1c] Bloomberg Law. NSO Loses Latest Challenge to Meta Lawsuit Over Whatsapp Spyware.

[1d] Bloomberg. Israeli Spyware Firm NSO Seen at Risk of Default as Sales Drop.

Or. en

Amendment 1111
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 153 b (new)

Motion for a resolution	*Amendment*
	153 b. NSO reportedly had revenues of $243 million in 2020. However, following the revelations by the Pegasus Project, the company faced several difficulties. Lawsuits filed by Apple and Meta against the company, blacklisting of NSO by the US Commerce department, the tightening of the Israeli export regime, critical inquiries in several countries, and internal frictions within the private equity fund behind NSO group, have led to a severe decline in profit. Reportedly, NSO Group's debt at one point even reached

6.5 times its normal revenues for a year.

Or. en

Amendment 1112
Sophia in 't Veld

Motion for a resolution
Paragraph 153 c (new)

Motion for a resolution	*Amendment*
	153 c. Pegasus spyware was initially sold to twenty-two end-users in fourteen EU Member States, using marketing and export licenses issued by Israel. Contracts with end-users in two Member States were subsequently terminated[1a]. It has not been confirmed which Member States are included in the list of fourteen, nor which two countries were removed. However, it is generally assumed the two are Poland and Hungary.
	[1a] Answers provided by NSO Group to PEGA secretariat following hearing, 20 July 2022.

Or. en

Amendment 1113
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 153 c (new)

Motion for a resolution	*Amendment*
	153 c. Pegasus spyware was initially sold to twenty-two end-users in fourteen EU Member States, using marketing and export licenses issued by Israel. Contracts with end-users in two Member States were

subsequently terminated. It has not been confirmed which Member States are included in the list of fourteen, nor which two countries were removed. However, it is generally assumed the two are Poland and Hungary.

Or. en

Amendment 1114
Sophia in 't Veld

Motion for a resolution
Paragraph 154 a (new)

Motion for a resolution	*Amendment*
	154 a. In March 2014, private equity fund Francisco Partners obtained a 70% stake in NSO Group. Under Francisco Partners, the company expanded its entities to different jurisdictions, including Cyprus, Bulgaria, the USA, the Netherlands and Luxembourg. During the Francisco Partners years between 2014 and 2019, the fund systematically reviewed the sale of NSO Group's products through the Business Ethics Committee (BEC). According to Francisco Partners, the BEC has denied tens of millions of dollars' worth of sales that would have otherwise be approved of under legal requirements[1a].
	[1a] Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.

Or. en

Amendment 1115
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 154 a (new)

Motion for a resolution	*Amendment*
	154 a. In March 2014, private equity fund Francisco Partners obtained a 70% stake in NSO Group. Under Francisco Partners, the company expanded its entities to different jurisdictions, including Cyprus, Bulgaria, the USA, the Netherlands and Luxembourg. During the Francisco Partners years between 2014 and 2019, the fund systematically reviewed the sale of NSO Group's products through the Business Ethics Committee (BEC). According to Francisco Partners, the BEC has denied tens of millions of dollars' worth of sales that would have otherwise be approved of under legal requirements.

Or. en

Amendment 1116
Sophia in 't Veld

Motion for a resolution
Paragraph 154 b (new)

Motion for a resolution	*Amendment*
	154 b. Francisco Partners sold their entire ownership interest, including that of the subsidiaries, on February 14, 2019 to Novalpina Capital. With this management buyout, the governance standards changed and the BEC was replaced by the Governance, Risk and Compliance Committee (GRCC) for the review of human rights records of potential customers[1a].
	[1a] Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.

Or. en

Amendment 1117
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 154 b (new)

Motion for a resolution	*Amendment*
	154 b. Francisco Partners sold their entire ownership interest, including that of the subsidiaries, on February 14, 2019 to Novalpina Capital. With this management buyout, the governance standards changed and the BEC was replaced by the Governance, Risk and Compliance Committee (GRCC) for the review of human rights records of potential customers.

Or. en

Amendment 1118
Sophia in 't Veld

Motion for a resolution
Paragraph 154 c (new)

Motion for a resolution	*Amendment*
	154 c. In line with the End Use/User Certificate after the tightening of the Israeli export regime, NSO Group has introduced a Human Rights Policy and a Human Rights Due Diligence (HRDD) procedure. As described in NSO Group's Transparency and Responsibility report of 2021, NSO group requires that all customer agreements include human rights compliance clauses and clauses outlining the suspension or termination of the use of NSO Group's products in case of human rights-related misuse. In a

written submission to PEGA, NSO Group confirmed that it has terminated contracts with EU Member States[1a], supposedly breaching the human rights clauses. Although it is not confirmed, it is assumed this decision concerns Poland and Hungary. NSO Group has not clarified if it has done an examination of the audit logs, and whether the customers in question had consented to such an examination. It is therefore not known if any evidence of the abuse still exists, if NSO has any way of preserving that evidence or if the Israeli authorities have any evidence.

[1a] PEGA Committee Hearing with NSO, 21 June 2022;

Or. en

Amendment 1119
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 154 c (new)

Motion for a resolution	*Amendment*
	154 c. In line with the End Use/User Certificate after the tightening of the Israeli export regime, NSO Group has introduced a Human Rights Policy and a Human Rights Due Diligence (HRDD) procedure. As described in NSO Group's Transparency and Responsibility report of 2021, NSO group requires that all customer agreements include human rights compliance clauses and clauses outlining the suspension or termination of the use of NSO Group's products in case of human rights-related misuse. In a written submission to PEGA, NSO Group confirmed that it has terminated contracts with EU Member States, supposedly

breaching the human rights clauses. Although it is not confirmed, it is assumed this decision concerns Poland and Hungary. NSO Group has not clarified if it has done an examination of the audit logs, and whether the customers in question had consented to such an examination. It is therefore not known if any evidence of the abuse still exists, if NSO has any way of preserving that evidence or if the Israeli authorities have any evidence.

Or. en

Amendment 1120
Sophia in 't Veld

Motion for a resolution
Paragraph 154 d (new)

Motion for a resolution	*Amendment*
	154 d. According to Amnesty International, the transparency report of NSO Group lacks a proper remediation policy for victims of unlawful surveillance and information on the ongoing lawsuits against NSO Group is absent[1a]. It becomes clear that NSO Group hides behind its Human Rights Policy and HRDD procedure as it spyware continues to be detected on devices of journalists and critics of authoritarian regimes[1b]. The reality tells the true story, not the corporate policies.

[1a] Amnesty International, NSO Group's new transparency report is 'another missed opportunity', press release, 1 July 2021

[1b] NYTimes. U.S. Blacklists Israeli Firm NSO Group Over Spyware.

Or. en

Amendment 1121
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 154 d (new)

Motion for a resolution	*Amendment*
	154 d. According to Amnesty International, the transparency report of NSO Group lacks a proper remediation policy for victims of unlawful surveillance and information on the ongoing lawsuits against NSO Group is absent. It becomes clear that NSO Group hides behind its Human Rights Policy and HRDD procedure as it spyware continues to be detected on devices of journalists and critics of authoritarian regimes. The reality tells the true story, not the corporate policies.

Or. en

Amendment 1122
Sophia in 't Veld

Motion for a resolution
Paragraph 155 a (new)

Motion for a resolution	*Amendment*
	155 a. NSO Group has confirmed that it exports its products from Bulgaria and Cyprus, but denies the export of the Pegasus spyware from these two countries in particular[1a]. Cyprus and Bulgaria have in addition denied having granted any export permits to NSO companies in general. As described in the chapters on Cyprus and Bulgaria, NSO subsidiaries often hide behind a different name in the national business registers. One of NSO's subsidiaries in Cyprus under the name of

Circles has however closed its offices in 2020[1b].

[1a] Amnesty International. Operating from the shadows. Inside NSO Group's corporate structure.

[1b] VICE. NSO Group Closes Cyprus Office of Spy Firm.

Or. en

Amendment 1123
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 155 a (new)

Motion for a resolution	*Amendment*
	155 a. NSO Group has confirmed that it exports its products from Bulgaria and Cyprus, but denies the export of the Pegasus spyware from these two countries in particular. Cyprus and Bulgaria have in addition denied having granted any export permits to NSO companies in general. As described in the chapters on Cyprus and Bulgaria, NSO subsidiaries often hide behind a different name in the national business registers. One of NSO's subsidiaries in Cyprus under the name of Circles has however closed its offices in 2020.

Or. en

Amendment 1124
Sophia in 't Veld

Motion for a resolution
Paragraph 156 a (new)

Motion for a resolution	*Amendment*
	156 a. In addition to ownership fall-outs, the US Commerce Department placed NSO Group on 3 November 2021 on a blacklist due to the incompatibility of NSO's activities with US foreign policy and national security concerns. The US administration prohibits the export of technology to NSO Group and its subsidiaries, de facto meaning that no American company can work with NSO Group[1a].
	[1a] NYTimes. U.S. Blacklists Israeli Firm NSO Group Over Spyware.

Or. en

Amendment 1125
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 156 a (new)

Motion for a resolution	*Amendment*
	156 a. In addition to ownership fall-outs, the US Commerce Department placed NSO Group on 3 November 2021 on a blacklist due to the incompatibility of NSO's activities with US foreign policy and national security concerns. The US administration prohibits the export of technology to NSO Group and its subsidiaries, de facto meaning that no American company can work with NSO Group.

Or. en

Amendment 1126
Sophia in 't Veld

Motion for a resolution
Paragraph 156 b (new)

Motion for a resolution	*Amendment*
	156 b. In response to the US Blacklisting, Credit Suisse, as one of the creditors of NSO Group, allegedly pushed the company to continue its sales of the Pegasus spyware to new customers. In a letter to BRG sent by Willkie Farr & Gallagher, several creditors stated that they were concerned that BRG was preventing NSO Group "from pursuing and obtaining new customers". One of the creditors - although not named in the letter - seems to be Credit Suisse. BRG responded to the lenders that it was deeply concerned about the pressing for NSO Group sales[1a].

[1a] Financial Times. Credit Suisse pushed for spyware sales at NSO despite US blacklisting.

Or. en

Amendment 1127
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 156 b (new)

Motion for a resolution	*Amendment*
	156 b. In response to the US Blacklisting, Credit Suisse, as one of the creditors of NSO Group, allegedly pushed the company to continue its sales of the Pegasus spyware to new customers. In a letter to BRG sent by Willkie Farr & Gallagher, several creditors stated that they were concerned that BRG was preventing NSO Group "from pursuing

and obtaining new customers". One of the creditors - although not named in the letter - seems to be Credit Suisse. BRG responded to the lenders that it was deeply concerned about the pressing for NSO Group sales.

Or. en

Amendment 1128
Sophia in 't Veld

Motion for a resolution
Paragraph 156 c (new)

Motion for a resolution	*Amendment*
	156 c. A few days after the US blacklisting of NSO, the United States Court of Appeals confirmed the proceeding of Meta's lawsuit against NSO, immediately followed by a complaint lodged at the federal court by Apple[1a]. In June 2022, the United States District Court rejected NSO Group's claim to immunity in the Apple lawsuit[1b]. At time of writing, the Apple lawsuit against NSO Group is still pending.
	[1a] NYTimes. Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones.
	[1b] https://www.docketalarm.com/cases/California_Northern_District_Court/3--21-cv-09078/Apple_Inc._v._NSO_Group_Technologies_Limited_et_al/35/

Or. en

Amendment 1129
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 156 c (new)

Motion for a resolution	*Amendment*
	156 c. A few days after the US blacklisting of NSO, the United States Court of Appeals confirmed the proceeding of Meta's lawsuit against NSO, immediately followed by a complaint lodged at the federal court by Apple. In June 2022, the United States District Court rejected NSO Group's claim to immunity in the Apple lawsuit. At time of writing, the Apple lawsuit against NSO Group is still pending.

Or. en

Amendment 1130
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 156 d (new)

Motion for a resolution	*Amendment*
	156 d. Around June 2022, a US defence contractor under the name of L3Harris was reportedly negotiating a deal with the NSO Group to take over NSO Groups' surveillance technology behind the Pegasus product as well as its personnel. Such a potential deal would have required the approval from both the US and Israeli government and had to meet the US Intelligence Services condition of selling Pegasus' software vulnerabilities and source code to the Five Eyes. According to a White House official, the deal would spur counterintelligence concerns and would not necessarily withdraw the company from the US blacklist. Due to such security concerns by the Biden administration, L3Harris terminated its

negotiations in July 2022.

Or. en

Amendment 1131
Sophia in 't Veld

Motion for a resolution
Paragraph 156 d (new)

Motion for a resolution	*Amendment*
	156 d. Despite of the US blacklisting, the Biden administration has allegedly appointed a former NSO advisor to an intelligence advisory board in October 2022. His name is Jeremy Bash. Under the auspices of Beacon Global Strategies, Bash was reportedly hired to advice NSO Group through Francisco Partners. According to the Guardian, he was one of the eight members on NSO's business ethics committee, allegedly providing him with a vote on the proceedings of proposed NSO sales. Beacon Global Strategies terminated the work with NSO after the pursued sales to Saudi Arabia[1a].
	[1a] The Guardian. Biden intelligence advisor previously vetted deals for Israeli NSO Group.

Or. en

Amendment 1132
Sophia in 't Veld

Motion for a resolution
Paragraph 156 e (new)

Motion for a resolution	*Amendment*
	156 e. NSO Group has similarly suffered from departing personnel. Since the murder on Jamal Khashoggi and the

growing concerns of the role of Pegasus therein, many employees have left NSO Group. Following these departures, Mr Hulio responded, "What worries me is the vibes of the employees."[1a] In August 2022, NSO Group announced to fire 100 employees[1b]. That same month, co-founder Shalev Hulio stepped down as CEO of NSO Group and was replaced by Yaron Shohat[1c]. NSO group changed policy and now focuses only on NATO members[1d].

[1a] The New Yorker. How Democracies spy on their citizens.

[1b] Calcalist. After cutbacks and CEO departure, what's next for the controversial NSO?

[1c] The Washington Post. CEO of Israeli NSO Spyware Company Steps Down Amid Shakeup; Calcalist. After cutbacks and CEO departure, what's next for the controversial NSO?

[1d] The Guardian. CEO of Israeli Pegasus spyware firm NSO to step down.

Or. en

Amendment 1133
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 156 e (new)

Motion for a resolution	*Amendment*
	156 e. Despite of the US blacklisting, the Biden administration has allegedly appointed a former NSO advisor to an intelligence advisory board in October 2022. His name is Jeremy Bash. Under the auspices of Beacon Global Strategies, Bash was reportedly hired to advice NSO Group through Francisco Partners.

According to the Guardian, he was one of the eight members on NSO's business ethics committee, allegedly providing him with a vote on the proceedings of proposed NSO sales. Beacon Global Strategies terminated the work with NSO after the pursued sales to Saudi Arabia.

Or. en

Amendment 1134
Sophia in 't Veld

Motion for a resolution
Paragraph 156 f (new)

Motion for a resolution	*Amendment*
	156 f. In October 2022, Shalev Hulio and former Chancellor of Austria Sebastian Kurz launched a new cybersecurity firm called "Dream Security". Mr Kurz stepped down as chancellor after a corruption scandal in October 2021 and started working for Peter Thiel's investment firm two months later. The company will produce solutions in the field of cyber incidents, centring on artificial intelligence, and will focus its sales on the European market[1a]. The cooperation between Kurz and Hulio constitutes an indirect but alarming connection between the spyware industry and Peter Thiel and his firm Palantir.
	[1a] OCCRP. Former Austrian Chancellor and ex-NSO Chief Start Cybersecurity Firm; The Times. Former NSO CEO and ex-Austrian Chancellor found startup.

Or. en

Amendment 1135
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja

on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 156 f (new)

Motion for a resolution	*Amendment*
	156 f. NSO Group has similarly suffered from departing personnel. Since the murder on Jamal Khashoggi and the growing concerns of the role of Pegasus therein, many employees have left NSO Group. Following these departures, Mr Hulio responded, "What worries me is the vibes of the employees." In August 2022, NSO Group announced to fire 100 employees. That same month, co-founder Shalev Hulio stepped down as CEO of NSO Group and was replaced by Yaron Shohat. NSO group changed policy and now focuses only on NATO members.

Or. en

Amendment 1136
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 156 g (new)

Motion for a resolution	*Amendment*
	156 g. In October 2022, Shalev Hulio and former Chancellor of Austria Sebastian Kurz launched a new cybersecurity firm called "Dream Security". Mr Kurz stepped down as chancellor after a corruption scandal in October 2021 and started working for Peter Thiel's investment firm two months later. The company will produce solutions in the field of cyber incidents, centring on artificial intelligence, and will focus its sales on the European market. The cooperation between Kurz and Hulio constitutes an indirect but alarming

connection between the spyware industry and Peter Thiel and his firm Palantir.

Or. en

Amendment 1137
Sophia in 't Veld

Motion for a resolution
Paragraph 156 g (new)

Motion for a resolution	*Amendment*
	156 g. Gil Dolev is a founding member of Dream Security. Gil Dolev is the brother of Shiri Dolev, NSO Group President. Gil Dolev also founded Wayout Group, a company specialised in intelligence gathering[1a]. Dream Security already raised $20 million from several investors, like Adi Shalev who was also involved in NSO investments. Other investors include Yevgeny Dibrov[1b], who represents 'the New Russian voice in what he calls 'the Russian-Israeli tech ecosystem'[1c].
	[1a] The Times of Israel. Former NSO CEO and ex-chancellor of Austria establish new cybersecurity startup.
	[1b] The Times. Former NSO CEO and ex-Austrian Chancellor found startup.
	[1c] Calcalist. From Russia, With Coding Skills.

Or. en

Amendment 1138
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 156 h (new)

Motion for a resolution	*Amendment*
	156 h. Gil Dolev is a founding member of Dream Security. Gil Dolev is the brother of Shiri Dolev, NSO Group President. Gil Dolev also founded Wayout Group, a company specialised in intelligence gathering. Dream Security already raised $20 million from several investors, like Adi Shalev who was also involved in NSO investments. Other investors include Yevgeny Dibrov, who represents 'the New Russian voice in what he calls 'the Russian-Israeli tech ecosystem'.

Or. en

Amendment 1139
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 157 a (new)

Motion for a resolution	*Amendment*
	157 a. Critically, it has also been uncovered that they are linked with NSO Group and Pegasus spyware. After much public pressure regarding NSO hiring Black Cube to target their opponents, former NSO CEO Shalev Hulio admitted to hiring Black Cube at in at least one situation in Cyprus.

Or. en

Amendment 1140
Sophia in 't Veld

Motion for a resolution
Paragraph 157 a (new)

Motion for a resolution	*Amendment*

157 a. Critically, it has also been uncovered that they are linked with NSO Group and Pegasus spyware. After much public pressure regarding NSO hiring Black Cube to target their opponents, former NSO CEO Shalev Hulio admitted to hiring Black Cube at in at least one situation in Cyprus.

Or. en

Amendment 1141
Sophia in 't Veld

Motion for a resolution
Paragraph 157 b (new)

Motion for a resolution	*Amendment*
	157 b. Black Cube got involved in Hungary during the 2018 elections, during which time they spied upon various NGOs and persons who had any connection to George Soros and reported back to Orban in order for him to spin their actives in a smear campaign[1a]. The resulting information from the surveillance of those individuals and NGOs appeared not only in the Hungarian state-controlled media, but also in the Jerusalem Post[1b].

[1a] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/ 6 July 2018.

[1b] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/ 6 July 2018.

Or. en

Amendment 1142
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 157 b (new)

Motion for a resolution	*Amendment*
	157 b. Black Cube got involved in Hungary during the 2018 elections, during which time they spied upon various NGOs and persons who had any connection to George Soros and reported back to Orban in order for him to spin their actives in a smear campaign.The resulting information from the surveillance of those individuals and NGOs appeared not only in the Hungarian state-controlled media, but also in the Jerusalem Post.

Or. en

Amendment 1143
Sophia in 't Veld

Motion for a resolution
Paragraph 158 a (new)

Motion for a resolution	*Amendment*
	158 a. All these vendors facilitate different systems. Whereas Cytrox is skilled in the extraction of data from mobile phones, Nexa technologies offers exploitation of global mobile communication systems. WiSpear can additionally extract data from Wi-Fi networks. The different vendors under Dilian's alliance thus allow for a broad assortment of software and services that Intellexa can offer and combine to its clients within and outside of the EU[1a].
	[1a] Haaretz. As Israel Reins in Its

Cyberarms Industry, an Ex-intel Officer is Building a New Empire.

Or. en

Amendment 1144
Sophia in 't Veld

Motion for a resolution
Paragraph 158 b (new)

Motion for a resolution	*Amendment*
	158 b. Parent company of Intellexa Alliance - Thalestris Limited - has different subsidiaries that have corporate presence throughout Ireland, Greece, the British Virgin Islands, Switzerland and Cyprus. Sara Aleksandra Hamou, reportedly the second ex-wife of Tal Dilian, has been the director of Thalestris Limited, and managing director of a subsidiary based in Greece[1a]. Hamou, originally born in Poland, holds a Cypriot passport issued by the Embassy of Poland in Cyprus[1b].
	[1a] Thalestris Limited. Annual Report and Consolidated Financial Statements for the period from 28 November 2019 to 31 December 2020.
	[1b] ReportersUnited. The Great Nephew and Big Brother.

Or. en

Amendment 1145
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 158 a (new)

Motion for a resolution	*Amendment*
	158 a. All these vendors facilitate different systems. Whereas Cytrox is skilled in the extraction of data from mobile phones, Nexa technologies offers exploitation of global mobile communication systems. WiSpear can additionally extract data from Wi-Fi networks. The different vendors under Dilian's alliance thus allow for a broad assortment of software and services that Intellexa can offer and combine to its clients within and outside of the EU.

Or. en

Amendment 1146
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 158 b (new)

Motion for a resolution	*Amendment*
	158 b. Parent company of Intellexa Alliance - Thalestris Limited - has different subsidiaries that have corporate presence throughout Ireland, Greece, the British Virgin Islands, Switzerland and Cyprus. Sara Aleksandra Hamou, reportedly the second ex-wife of Tal Dilian, has been the director of Thalestris Limited, and managing director of a subsidiary based in Greece. Hamou, originally born in Poland, holds a Cypriot passport issued by the Embassy of Poland in Cyprus.

Or. en

Amendment 1147
Sophia in 't Veld

Motion for a resolution
Paragraph 159 a (new)

Motion for a resolution	*Amendment*
	159 a. In 2017, Cytrox Holdings Zrt. was founded in North Macedonia by Ivo Malinkovski. However, the cradle of Cytrox was actually in Tel Aviv, and Malinkovski was just the front man. After the Pegasus Project revelations, Malinkovski tried to erase all traces connecting him to Cytrox. (Unsuccessfully, as he left a picture of himself holding a coffee mug with "Cytrox" on it). There were rumours that the person actually in charge is Ivo's father Ilija Malinkovski. Today he owns a restaurant and wine chateau, but since the 1990s he also has a company selling weapons[1a], which is interestingly also mentioned on the website of the Greek ministry of Foreign Affairs[1b].

1a

https://balkaninsight.com/2022/01/06/wine-weapons-and-whatsapp-a-skopje-spyware-scandal/

1b

http://www2.mfa.gr/en/companies/company/1093

Or. en

Amendment 1148
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 159 a (new)

Motion for a resolution	*Amendment*
	159 a. In 2017, Cytrox Holdings Zrt. was founded in North Macedonia by Ivo Malinkovski. However, the cradle of

Cytrox was actually in Tel Aviv, and Malinkovski was just the front man. After the Pegasus Project revelations, Malinkovski tried to erase all traces connecting him to Cytrox. (Unsuccessfully, as he left a picture of himself holding a coffee mug with "Cytrox" on it). There were rumours that the person actually in charge is Ivo's father Ilija Malinkovski. Today he owns a restaurant and wine chateau, but since the 1990s he also has a company selling weapons, which is interestingly also mentioned on the website of the Greek ministry of Foreign Affairs.

Or. en

Amendment 1149
Sophia in 't Veld

Motion for a resolution
Paragraph 159 b (new)

Motion for a resolution	*Amendment*
	159 b. Cytrox was the developer of the Predator spyware. In contrast to Pegasus spyware, Predator requires the target to click on a link to install the software[1a]. When Cytrox was on the verge of bankruptcy, Tal Dilian rescued it with the acquisition costing under 5 million dollars[1b]. Cytrox was subsequently merged with Dilian's WiSpear[1c]. This acquisition added the Predator spyware to the arsenal of Intellexa technologies.
	[1a] European Parliament. Greece's Predatorgate. The latest chapter in Europe's spyware scandal?
	[1b] BalkanInsight. Wine, Weapons and Whatsapp: A Skopje Spyware Scandal.
	[1c] Pitchbook. Cytrox overview.

Or. en

Amendment 1150
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 159 b (new)

Motion for a resolution	*Amendment*
	159 b. Cytrox was the developer of the Predator spyware. In contrast to Pegasus spyware, Predator requires the target to click on a link to install the software. When Cytrox was on the verge of bankruptcy, Tal Dilian rescued it with the acquisition costing under 5 million dollars. Cytrox was subsequently merged with Dilian's WiSpear. This acquisition added the Predator spyware to the arsenal of Intellexa technologies.

Or. en

Amendment 1151
Sophia in 't Veld

Motion for a resolution
Paragraph 159 c (new)

Motion for a resolution	*Amendment*
	159 c. According to CitizenLab, several Cytrox companies have been registered in Israel - Cytrox EMEA ltd. and Cytrox Software Ltd. - and in Hungary as Cytrox Holdings Zrt.[1a] All of the shares of Cytrox Holdings Zrt. and Cytrox EMEA ltd - later renamed to Balinese Ltd. - were transferred to Aliada Group Inc. as registered in the British Virgin Islands. Aliada Group is also the owner of WiSpear. The main shareholders of Aliada Group are Dilian himself, as well as Oz Liv, Meir Shamir and Avi Rubinstein. In December 2020,

Rubinstein lodged a complaint against his co-shareholders of Aliada Group for the illegal dilution of his shares. According to the lawsuit, the relocation of shares to the British Virgin Islands and later to Ireland circumvented Israeli and foreign export control laws[1b].

[1a] Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware.

[1b] Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware.

Or. en

Amendment 1152
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 159 c (new)

Motion for a resolution	*Amendment*
	159 c. According to CitizenLab, several Cytrox companies have been registered in Israel - Cytrox EMEA ltd. and Cytrox Software Ltd. - and in Hungary as Cytrox Holdings Zrt. All of the shares of Cytrox Holdings Zrt. and Cytrox EMEA ltd - later renamed to Balinese Ltd. - were transferred to Aliada Group Inc. as registered in the British Virgin Islands. Aliada Group is also the owner of WiSpear. The main shareholders of Aliada Group are Dilian himself, as well as Oz Liv, Meir Shamir and Avi Rubinstein. In December 2020, Rubinstein lodged a complaint against his co-shareholders of Aliada Group for the illegal dilution of his shares. According to the lawsuit, the relocation of shares to the British Virgin Islands and later to Ireland circumvented Israeli and foreign export

control laws.

Or. en

Amendment 1153
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 159 d (new)

Motion for a resolution	*Amendment*
	159 d. On 16 December 2021, CitizenLab released a report stating likely Predator customers were found in Armenia, Egypt, Greece, Indonesia, Madagascar, Oman, Saudi Arabia, and Serbia[314a].
	[314a] CitizenLab: Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware. https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

Or. en

Amendment 1154
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 159 e (new)

Motion for a resolution	*Amendment*
	159 e. According to experts' reporting the Predator spyware has apparently been abused by third countries with a poor human rights record to target government critics. For example, CitizenLab found

that in June 2021 two Egyptians - exiled politician Ayman Nour and the host of a popular news program - were hacked with Predator spyware. The phone of Ayman Nour was simultaneously infected with both Cytrox's Predator and NSO Group's Pegasus spyware, operated by two different government clients[314b].

[314b] CitizenLab: Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware. https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

Or. en

Amendment 1155
Hannah Neumann, Saskia Bricmont, Gwendoline Delbos-Corfield, Diana Riba i Giner, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 159 f (new)

Motion for a resolution	*Amendment*
	159 f. On 30 November 2022, an investigative report by Lighthouse Reports, in collaboration with the Israeli newspaper Haaretz and the Greek outlet Inside Story, revealed that the EU-based company Intellexa Alliance secretly and illegally delivered the spyware Predator in May this year to the Sudanese Rapid Support Force militia by a Cessna private jet. The Rapid Support Forces militia is infamous for its alleged war crimes in the Western Darfur region and its suppression of pro-democracy protests. Flight records linked the private jet, flying in and out via Cyprus, to Tal Dilian, a former senior Israel Defence Force operative who set up Intellexa Alliance in 2019 with bases in Cyprus and Greece[314c].

[314c] ***Lighthouse Reports, Flight of the Predator https://www.lighthousereports.nl/investigation/flight-of-the-predator/***

Or. en

Amendment 1156
Sophia in 't Veld

Motion for a resolution
Paragraph 161

Motion for a resolution	*Amendment*
161. Poltrex was launched in October 2018 and the sole shareholder of the company was Intellexa ltd as registered in the British Virgin Islands. Israeli Shahak Avni - founder of the Cypriot NCIS Intelligence Services ltd[315] and associate of Tal Dilian - was registered as the director of Poltrex in September 2019. In October 2019, both Avni and Dilian became co-directors and the name of Poltrex was changed to Alchemycorp Ltd. Notwithstanding the renaming of Poltrex, the company was still hosted in the Novel Tower - the same location as the address of WiSpear[316] .	161. Poltrex was launched in October 2018 and the sole shareholder of the company was Intellexa ltd as registered in the British Virgin Islands. Israeli Shahak Avni - founder of the Cypriot NCIS Intelligence Services ltd[315] and associate of Tal Dilian - was registered as the director of Poltrex in September 2019. In October 2019, both Avni and Dilian became co-directors and the name of Poltrex was changed to Alchemycorp Ltd. Notwithstanding the renaming of Poltrex, the company was still hosted in the Novel Tower - the same location as the address of WiSpear[316] .
[315] Philenews. ***FILE: The state insulted Avni and Dilian.***	[315] Philenews. ***ΦΑΚΕΛΟΣ: Η Πολιτεία υπέθαλπε Άβνι και Ντίλιαν***
[316] CyprusMail. Akel says found ‘smoking gun’ linking Cyprus to Greek spying scandal.	[316] CyprusMail. Akel says found ‘smoking gun’ linking Cyprus to Greek spying scandal.

Or. en

Amendment 1157
Sophia in 't Veld

Motion for a resolution

Paragraph 161 a (new)

Motion for a resolution	*Amendment*
	161 a. When the investigations surrounding Dilian's spyware van were proceeding, the ownership of Alchemycorp Ltd. was transferred to Yaron Levgoren. Levgoren was an employee of Cytrox Holdings[1a]. According to his LinkedIn he currently represents the Intellexa company Apollo Technologies, based in Greece.
	[1a] Philenews. How the spyware scandal in Greece is related to Cyprus.

Or. en

Amendment 1158
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 161 a (new)

Motion for a resolution	*Amendment*
	161 a. When the investigations surrounding Dilian's spyware van were proceeding, the ownership of Alchemycorp Ltd. was transferred to Yaron Levgoren. Levgoren was an employee of Cytrox Holdings. According to his LinkedIn he currently represents the Intellexa company Apollo Technologies, based in Greece.

Or. en

Amendment 1159
Sophia in 't Veld

Motion for a resolution

Subheading 118 a (new)

Motion for a resolution	*Amendment*
	Verint/Cognyte

Or. en

Amendment 1160
Sophia in 't Veld

Motion for a resolution
Paragraph 161 b (new)

Motion for a resolution	*Amendment*
	161 b. Verint is an Israeli-American cyber company that has many subsidiaries all over the world. In Europe alone, Verint is registered as of 2021 in Bulgaria, the Netherlands, Cyprus, Germany and France. Verint also had subsidiaries operating under the name Cognyte. These subsidiaries operate independently since 2021 when Verint concluded the spin-off of its intelligence and cyber activities to Cognyte[1a]. Cognyte's European subsidiaries are registered in Cyprus (UTX Technologies), Bulgaria (Cognyte Bulgaria EOOD), the Netherlands (Cognyte Netherlands B.V.), Germany (Syborg GmbH, Syborg Grundbesitz GmbH and Syborg Informationsysteme b.h. OHG) and Romania (Cognyte Romania S.R.L.)[1b].

[1a] Calcalistech. Verint completes spinn-off of its defense activities into new company Cognyte Software.

[1b] https://www.sec.gov/Archives/edgar/data/1824814/000182481421000007/exhibit81.htm

Or. en

Amendment 1161
Sophia in 't Veld

Motion for a resolution
Paragraph 161 c (new)

Motion for a resolution	*Amendment*
	161 c. Verint has sold surveillance tools to several repressive governments, amongst others in Azerbaijan, Indonesia and in South Sudan. In the case of the latter, the Sudanese National Security Service (NSS) used Verint's interception equipment against human rights activists and journalists between March 2015 and February 2017. According to an Amnesty International inquiry, local mobile operator Vivacell Network of the World enabled the NSS to listen in on all Sudanese telecommunications[1a]. Verint did not respond to questions from Amnesty, but did publish a statement outlining how Verint's independently functioning unit Cognyte is in fact the defence unit whereas Verint solely deals with customer engagement. According to Verint, the division with Cognyte was already in place for many years before the official spin-off in 2021, distancing themselves from the alleged export of surveillance equipment to countries with poor human rights records[1b].
	[1a] Haaretz. Israeli Cyber Firm Sold Spytech to South Sudan, Investigation Finds; Amnesty International. South Sudan: Rampant abusive surveillance by NSS instils climate of fear.
	[1b] Haaretz. Israeli Cyber Firm Sold Spytech to South Sudan, Investigation Finds;

Or. en

Amendment 1162
Sophia in 't Veld

Motion for a resolution
Paragraph 161 d (new)

Motion for a resolution	*Amendment*
	161 d. Cognyte also has a history of exports to countries with poor human rights records. A 2021 Meta inquiry identified customers in Israel, Serbia, Colombia, Kenya, Morocco, Mexico, Jordan, Thailand and Indonesia[1a]. Cognyte subsidiary UTX Technologies, registered in Cyprus, reportedly also received licenses for the export of monitoring software to Mexico, United Arab Emirates, Nigeria, Israel, Peru, Colombia, Brazil, South Korea and Thailand between September 2014 and March 2015[1b]. Four of these countries overlap with Cognyte customers identified in the 2021 Meta report. In addition, UTX Technologies secured an agreement with Bangladesh for a Web Intelligence System for 2 million dollars in 2019 and for a cellular tracking system for 500.000 dollar in 2021[1c].
	[1a] Meta. Threat Report on the Surveillance-for-Hire Industry.
	[1b] Philenews. Cyprus is a pioneer in software exports (documents).
	[1c] Haaretz. Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Records.

Or. en

Amendment 1163
Sophia in 't Veld

Motion for a resolution
Paragraph 161 e (new)

Motion for a resolution	*Amendment*

161 e. On January 15 2023, media reported that Israel's Cognyte Software Ltd won a tender for the sale of its interception spyware to Myanmar, one month prior to the military coup that took place in February 2021. The purchase of Cognyte's spyware by Myanmar was officially placed on 30 December 2020[1a].

[1a] Reuters. Israel's Cognyte won tender to sell intercept spyware to Myanmar before coup- documents.

Or. en

Amendment 1164
Sophia in 't Veld

Motion for a resolution
Paragraph 161 f (new)

Motion for a resolution	*Amendment*
	161 f. Next to the export to third countries, Cognyte has also facilitated the transport of tracking equipment to Member States. Through UTX Technologies, registered in Cyprus, Gi2 technology was shipped to another Cognyte subsidiary in Germany under the name of Syborg Informationsysteme[1a]. This Gi2 technology was reportedly also sent to a Verint subsidiary in Poland "for demonstrations purposes". Gi2 technology has the ability to gain access to a particular device and can even impersonate the owner and send false messages through this same device[1b]. These shipments took place between 2013 and 2014. At that time Verint and Cognyte were still part of the same company structure.

[1a] https://www.sec.gov/Archives/edgar/data/1824814/000119312521008526/d52351dex

81.htm

[1b] Philenews. Cyprus is a pioneer in software exports (documents)

Or. en

Amendment 1165
Sophia in 't Veld

Motion for a resolution
Paragraph 161 g (new)

Motion for a resolution	*Amendment*
	161 g. UTX Technologies also sold monitoring systems in 2013 to a French export company under the name of COFREXPORT[1a]. This company has ceased operations and is closed at time of writing.
	[1a] Philenews. Cyprus is a pioneer in software exports (documents)

Or. en

Amendment 1166
Sophia in 't Veld

Motion for a resolution
Paragraph 161 h (new)

Motion for a resolution	*Amendment*
	161 h. Like many other spyware vendors, Cognyte's company structure is highly complex, due to name changes, divisions and spin-offs overtime. The Cognyte subsidiaries show however that EU Member States are not only used to export surveillance equipment from, but also function as a foothold to sell and ship surveillance equipment within Europe. Israeli spyware companies thus benefit from the EU's internal market,

facilitating the transport of their equipment to both their own subsidiaries as well as to new companies registered in EU Member States.

Or. en

Amendment 1167
Sophia in 't Veld

Motion for a resolution
Paragraph 162 a (new)

Motion for a resolution	*Amendment*
	162 a. According to a TheMarker inquiry, Candiru now also offers spyware to break into mobile devices[1a]. It solely sells its spyware to governments and its clientele consists of "Europe, the former Soviet Union, the Persian Gulf, Asia and Latin America"[1b]. As highlighted in the chapter on Spain, four people out of the 65 victims were targeted with Candiru, and at least two people were targeted with both Candiru and Pegasus[1c].

[1a] Haaretz. Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed.

[1b] CitizenLab. Hooking Candiru. Another Mercenary Spyware Vendor Comes into Focus.

[1c] CitizenLab. CatalanGate. Extensive Mercenary Spyware Operations against Catalans Using Pegasus and Candiru.

Or. en

Amendment 1168
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 162 a (new)

Motion for a resolution	*Amendment*
	162 a. According to a TheMarker inquiry, Candiru now also offers spyware to break into mobile devices. It solely sells its spyware to governments and its clientele consists of "Europe, the former Soviet Union, the Persian Gulf, Asia and Latin America". As highlighted in the chapter on Spain, four people out of the 65 victims were targeted with Candiru, and at least two people were targeted with both Candiru and Pegasus.

Or. en

Amendment 1169
Sophia in 't Veld

Motion for a resolution
Paragraph 162 b (new)

Motion for a resolution	*Amendment*
	162 b. As with the other spyware vendors, corporate obfuscation lays at the heart of this company, as it has undergone several name changes throughout the last couple of years. The company has changed it names to DF Associates Ltd. in 2017, Grindavik Solutions Ltd in 2018, Taveta Ltd in 2019 and the most recent change to Saito Tech Ltd in 2020[1a]. For sake of clarity, we will refer to the company as Candiru.
	[1a] CitizenLab. Hooking Candiru. Another Mercenary Spyware Vendor Comes into Focus.

Or. en

Amendment 1170
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 162 b (new)

Motion for a resolution	*Amendment*
	162 b. As with the other spyware vendors, corporate obfuscation lays at the heart of this company, as it has undergone several name changes throughout the last couple of years. The company has changed it names to DF Associates Ltd. in 2017, Grindavik Solutions Ltd in 2018, Taveta Ltd in 2019 and the most recent change to Saito Tech Ltd in 2020. For sake of clarity, we will refer to the company as Candiru.

Or. en

Amendment 1171
Sophia in 't Veld

Motion for a resolution
Paragraph 162 c (new)

Motion for a resolution	*Amendment*
	162 c. Just like NSO Group, Candiru was similarly placed on the US blacklist by the US Commerce Department in November 2021. It is speculated that the reason for Candiru's blacklisting is the fact that CEO of NSO Group Shalev Hulio allegedly was a secret partner in Candiru and introduced the company to important middlemen in the intelligence world. Reportedly, Mr Hulio would even argue that Candiru's product is actually a repackaging of Pegasus[1a]. At a later stage Hulio and Candiru became rivals, as Hulio heard from Francisco Partners that Candiru wanted to compete with NSO Group[1b]. On July 1 2022, security

researchers identified a novel Chrome zero-day exploit that was used by Candiru to target individuals in Lebanon, Palestine, Yemen and Turkey[1c]. The exploit was addressed by Google and has since also been patched by Microsoft and Apple[1d].

[1a] Haaretz. 'We're on the U.S. Blacklist Because of You': The Dirty Clash Between Israeli Cyberarms Makers

[1b] Haaretz. 'We're on the U.S. Blacklist Because of You': The Dirty Clash Between Israeli Cyberarms Makers

[1c] TechCrunch. Spyware maker Candiru linked to Chrome zero-day targeting journalists.

[1d] The HackerNews. Candiru Spyware Caught Exploiting Google Chrome Zero-Day to Target Journalists.

Or. en

Amendment 1172
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 162 c (new)

Motion for a resolution	*Amendment*
	162 c. Just like NSO Group, Candiru was similarly placed on the US blacklist by the US Commerce Department in November 2021. It is speculated that the reason for Candiru's blacklisting is the fact that CEO of NSO Group Shalev Hulio allegedly was a secret partner in Candiru and introduced the company to important middlemen in the intelligence world. Reportedly, Mr Hulio would even argue that Candiru's product is actually a repackaging of Pegasus. At a later stage Hulio and Candiru became rivals, as

Hulio heard from Francisco Partners that Candiru wanted to compete with NSO Group. On July 1 2022, security researchers identified a novel Chrome zero-day exploit that was used by Candiru to target individuals in Lebanon, Palestine, Yemen and Turkey. The exploit was addressed by Google and has since also been patched by Microsoft and Apple.

Or. en

Amendment 1173
Sophia in 't Veld

Motion for a resolution
Paragraph 163 a (new)

Motion for a resolution	*Amendment*
	163 a. Lighthouse Report's investigation also highlighted the role of the telecom industry, where the leasing of phone network access points or "global titles" allows for this abuse to continue. According to GSM Association, the industry organisation representing mobile network operators worldwide, phone operators cannot always identify the source and purpose of the traffic that flows through their networks, which makes it difficult to halt these practices[1a].
	1a https://www.lighthousereports.nl/investigation/revealing-europes-nso/

Or. en

Amendment 1174
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 163 a (new)

Motion for a resolution	*Amendment*
	163 a. Lighthouse Report's investigation also highlighted the role of the telecom industry, where the leasing of phone network access points or "global titles" allows for this abuse to continue. According to GSM Association, the industry organisation representing mobile network operators worldwide, phone operators cannot always identify the source and purpose of the traffic that flows through their networks, which makes it difficult to halt these practices.

Or. en

Amendment 1175
Sophia in 't Veld

Motion for a resolution
Paragraph 163 b (new)

Motion for a resolution	*Amendment*
	163 b. Tykelab is a part of RCS Lab, an Italian company known for its interception activities in Italy and abroad, which was brought to light by an announcement of a third company, Cy4Gate, which acquired RCS Lab. RCS Lab has off-shoots in France, Germany and Spain[1a]. RCS Lab has another concealed subsidiary, Azienda Informatica Italiana, which builds interception software for Android and iPhone devices[1b].
	[1a] https://euobserver.com/digital/155849
	[1b] https://www.lighthousereports.nl/investigation/revealing-europes-nso/

Or. en

Amendment 1176
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 163 b (new)

Motion for a resolution	*Amendment*
	163 b. Tykelab is a part of RCS Lab, an Italian company known for its interception activities in Italy and abroad, which was brought to light by an announcement of a third company, Cy4Gate, which acquired RCS Lab. RCS Lab has off-shoots in France, Germany and Spain. RCS Lab has another concealed subsidiary, Azienda Informatica Italiana, which builds interception software for Android and iPhone devices.

Or. en

Amendment 1177
Sophia in 't Veld

Motion for a resolution
Paragraph 164 a (new)

Motion for a resolution	*Amendment*
	164 a. A Threat Intelligence Researcher of cyber security firm Lookout, Justin Albrecht, said that although Hermit's method of installation was less sophisticated than that of Pegasus, its capabilities were similar. Hermit needs a phone user to click on an infected link for it to compromise a device[1a].
	[1a] https://euobserver.com/digital/155849

Or. en

Amendment 1178
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 164 a (new)

Motion for a resolution	*Amendment*
	164 a. A Threat Intelligence Researcher of cyber security firm Lookout, Justin Albrecht, said that although Hermit's method of installation was less sophisticated than that of Pegasus, its capabilities were similar. Hermit needs a phone user to click on an infected link for it to compromise a device.

Or. en

Amendment 1179
Sophia in 't Veld

Motion for a resolution
Paragraph 164 b (new)

Motion for a resolution	*Amendment*
	164 b. According to RCS Lab, "any sales or implementation of products is performed only after receiving an official authorisation from the competent national authorities. The products supplied to customers are installed at their facilities, and RCS Lab personnel are not permitted under any circumstances to carry out operational activities in support of the customer or to have access to the processed data. Due to binding confidentiality agreements, RCS Lab cannot disclose any details about its customers. The Cy4gate Group, of which RCS Lab is a member, adheres to the UN Global Compact and therefore condemns all forms of human rights violations. RCS

Lab's products are provided with a clear, specific, and exclusive purpose: to support law enforcement agencies in the prevention and suppression of heinous crimes."[1a] However, it is not possible to verify if Cy4gate Group, including RCS Lab, adheres to its own declared standards.

[1a] https://euobserver.com/digital/155849

Or. en

Amendment 1180
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 164 b (new)

Motion for a resolution	*Amendment*
	164 b. According to RCS Lab, "any sales or implementation of products is performed only after receiving an official authorisation from the competent national authorities. The products supplied to customers are installed at their facilities, and RCS Lab personnel are not permitted under any circumstances to carry out operational activities in support of the customer or to have access to the processed data. Due to binding confidentiality agreements, RCS Lab cannot disclose any details about its customers. The Cy4gate Group, of which RCS Lab is a member, adheres to the UN Global Compact and therefore condemns all forms of human rights violations. RCS Lab's products are provided with a clear, specific, and exclusive purpose: to support law enforcement agencies in the prevention and suppression of heinous crimes." However, it is not possible to verify if Cy4gate Group, including RCS Lab, adheres to its own declared

standards.

Or. en

Amendment 1181
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 164 c (new)

Motion for a resolution	*Amendment*
	164 c. According to an investigation from Lighthouse Reports published in August 2022, Tykelab's surveillance tool Hermit was used to target individuals around the world, including in Libya, Nicaragua, Malaysia, Costa Rica, Iraq, Mali, Greece and Portugal – as well as in Italy itself[325a].
	[325a] Lighthouse Reports: Revealing Europe's NSO. https://www.lighthousereports.nl/investigation/revealing-europes-nso/

Or. en

Amendment 1182
Sophia in 't Veld

Motion for a resolution
Paragraph 165 a (new)

Motion for a resolution	*Amendment*
	165 a. DSIRF developed spyware called Subzero/KNOTWEED, which can be deployed using zero-day vulnerabilities in Windows and Adobe Reader, and which - according to its own advertising - can be secretly installed on the target device. Once installed, Subzero takes "full control of the target computer" and

provides "complete access to all data and passwords". Subzero customers can extract passwords, take screenshots, view current and previous locations, and "access, download, modify and upload files on the target computer" via a web interface. DSIRF promotes Subzero as "next-generation cyber warfare", saying the tool was "designed for the cyber age"[1a]. In 2020 DSIRF valued its software Subzero with 245 million euros.

[1a] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/

Or. en

Amendment 1183
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 165 a (new)

Motion for a resolution	*Amendment*
	165 a. DSIRF developed spyware called Subzero/KNOTWEED, which can be deployed using zero-day vulnerabilities in Windows and Adobe Reader, and which - according to its own advertising - can be secretly installed on the target device. Once installed, Subzero takes "full control of the target computer" and provides "complete access to all data and passwords". Subzero customers can extract passwords, take screenshots, view current and previous locations, and "access, download, modify and upload files on the target computer" via a web interface. DSIRF promotes Subzero as "next-generation cyber warfare", saying the tool was "designed for the cyber age". In 2020 DSIRF valued its software Subzero with 245 million euros.

Amendment 1184
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 165 b (new)

Motion for a resolution	*Amendment*
	165 b. The connection with Russia became clear from links of several high level staff members of DSIRF. The owner of DSIRF is Peter Dietenberger, a "man with best connections in the Kremlin" and a "door opener of western companies in Putin's empire". Dietenberger lived several years in Russia, had a Russian company and several Russian business partners. One of his Russian business partners, Boris Vasilyev, was also in the board of directors of DSIRF. DSIRF names several references for its firm and products: Michael Harms (CEO of the German Eastern Business Association), Stephan Fanderl (Chairman of the Board of Galeria Karstadt Kaufhof, who wanted to bring Walmart to Russia), Christian Kremer (former President of BMW in Russia and CEO of Russian Machines, which is sanctioned by the US since 2018) and Florian Schneider (partner at the large business law firm Dentons in Moscow). "Russian Machines", a company owned by the oligarch Oleg Deripaska, is said to be using the services of DSIRF. The powerful local entrepreneur Siegfried "Sigi" Wolf, who advised the party of thes former Chancellor Sebastian Kurz on economic issues, is considered a confidante of Deripaska. Also Jan Marsalek, an alleged criminal wanted on an Interpol arrest warrant for commercial fraud charges amounting to billions, among other financial and economic offenses, is

involved. In August 2018, he received an email from Florian Stermann (Secretary General of the Russian-Austrian Friendship Society, and considered in investigations by the public prosecutor's office to be a "confidant" of the FPÖ) with a company presentation, initially intended for the Austrian Ministry of Interior[327a], of DSIRF. Already in 2013, he allegedly tried to sell spyware of the Italian company Hacking Team to Grenada. He is said to hide in Moscow at the moment, under the care of the FSB, the Russian secret service.The first office of DSIRF belonged to the then SPÖ chancellor of Austria Christian Kern. Kern and his wife Evelyn Steinberger-Kern bought this loft for one million euros at exactly the time when DSIRF moved in as a tenant.

327a

https://www.diepresse.com/6201008/justiz-ermittelt-gegen-wiener-staatstrojaner-schoepfer

Or. en

Amendment 1185
Sophia in 't Veld

Motion for a resolution
Paragraph 165 b (new)

Motion for a resolution	*Amendment*
	165 b. The connection with Russia become clear from links of several high level staff members of DSIRF. The owner of DSIRF is Peter Dietenberger, a "man with best connections in the Kremlin" and a "door opener of western companies in Putin's empire"[1a]. Dietenberger lived several years in Russia, had a Russian company and several Russian business partners. One of his Russian business partners, Boris Vasilyev, was also in the

board of directors of DSIRF. DSIRF names several references for its firm and products: Michael Harms (CEO of the German Eastern Business Association), Stephan Fanderl (Chairman of the Board of Galeria Karstadt Kaufhof, who wanted to bring Walmart to Russia), Christian Kremer (former President of BMW in Russia and CEO of Russian Machines, which is sanctioned by the US since 2018) and Florian Schneider (partner at the large business law firm Dentons in Moscow)[1b]. "Russian Machines", a company owned by the oligarch Oleg Deripaska, is said to be using the services of DSIRF. The powerful local entrepreneur Siegfried "Sigi" Wolf, who advised former Chancellor Sebastian Kurz on economic issues, is considered a confidante of Deripaska[1c]. Also Jan Marsalek, an alleged criminal wanted on an Interpol arrest warrant for commercial fraud charges amounting to billions, among other financial and economic offenses, is involved. In August 2018, he received an email from Florian Stermann (Secretary General of the Russian-Austrian Friendship Society, and considered in investigations by the public prosecutor's office to be a "confidant" of the FPÖ)[1d] with a company presentation of DSIRF. Already in 2013, he allegedly tried to sell spyware of the Italian company Hacking Team to Grenada. He is said to hide in Moscow at the moment, under the care of the FSB, the Russian secret service[1e]. The first office of DSIRF belonged to the then SPÖ chancellor of Austria Christian Kern. Kern and his wife Evelyn Steinberger-Kern bought this loft for one million euros at exactly the time when DSIRF moved in as a tenant[1f].

[1a] https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html

[1b] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/

[1c] https://www.derstandard.at/story/2000131301583/causa-marsalek-die-verbindungen-einer-spionagefirma-werfen-fragen-auf

[1d] https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html

[1e] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/; https://www.dw.com/en/wanted-wirecard-executive-jan-marsalak-reportedly-hiding-in-moscow/a-61440213

[1f] https://www.tagesanzeiger.ch/software-zur-gesichtserkennung-von-shoppern-467623717263

Or. en

Amendment 1186
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 165 c (new)

Motion for a resolution	*Amendment*
	165 c. In July 2022, Microsoft found out that Subzero was used during unauthorised, malicious activity to attack ten law firms, banks, and strategic consultancies in Austria, the United Kingdom and Panama. Austria currently has no legal basis for the unauthorised deployment of spyware like Subzero by public authorities, and it is also illegal if one private company would use it against another. According to the Austrian

Directorate for state security and intelligence (DSN), a department of the Austrian Ministry of Interior, Austria currently does not only lack the means in its executive to fight cybercrimes but also the appropriate judicial powers to address criminal activity in this area[327b]. Following the Microsoft publication, on 28 July 2022, the Austrian digital rights NGO Epicenter.works filed a criminal complaint against DSIRF at the Vienna Public Prosecutor's Office for unlawful access to a computer system, data damage, interference with the functioning of computer systems, fraudulent misuse of data processing, criminal organisation and violation of the Foreign Trade and Payments Act with regards to Dual Use Goods. On 7 October 2022, the Austrian Federal Ministry of Labour and Economi c Affairs stated that it had not issued an export license to DSIRF, and according to the Austrian Federal Ministry for Justice Affairs, the Vienna Public Prosecutor's Office has started a criminal investigation into DSIRF. The use of the Subzero spyware against unknowing targets in Austria means that either a private or public authority in Austria has applied the software illegally, the software was used by a foreign actor and export restrictions were violated by DSIRF or the software was exported to another Member State and used from there legally or illegally against an Austrian target. The investigation is still ongoing.

327b

https://www.diepresse.com/6219330/staatstrojaner-subzero-anwaelte-bespitzelt-mit-geheimdiensten-verhandelt?

Or. en

Amendment 1187
Sophia in 't Veld

Motion for a resolution
Paragraph 165 c (new)

Motion for a resolution	*Amendment*
	165 c. In July 2022, Microsoft found out that Subzero was used during unauthorised, malicious activity to attack law firms, banks, and strategic consultancies in Austria, the United Kingdom and Panama[1a]. Austria currently has no legal basis for the unauthorised deployment of spyware like Subzero by public authorities, and it is also illegal if one private company would use it against another. Following the Microsoft publication, on 28 July 2022, the Austrian digital rights NGO Epicenter.works filed a criminal complaint against DSIRF at the Vienna Public Prosecutor's Office for unlawful access to a computer system, data damage, interference with the functioning of computer systems, fraudulent misuse of data processing, criminal organisation and violation of the Foreign Trade and Payments Act with regards to Dual Use Goods[1b]. On 7 October 2022, the Austrian Federal Ministry of Labour and Economic Affairs stated that it had not issued an export license to DSIRF[1c], and according to the Austrian Federal Ministry for Justice Affairs, the Vienna Public Prosecutor's Office has started a criminal investigation into DSIRF[1d]. The use of the Subzero spyware against targets in Austria means that either a private or public authority in Austria has applied the software illegally, the software was used by a foreign actor and export restrictions were violated by DSIRF or the software was exported to another Member State and used from there legally or illegally against an Austrian target. The investigation is still ongoing.
	[1a] https://www.microsoft.com/en-us/security/blog/2022/07/27/untangling-knotweed-european-private-sector-

offensive-actor-using-0-day-exploits/

[1b]

https://en.epicenter.works/document/4236

[1c] Response by Martin Kocher, Federal Minister for Digital and Economic Affairs of Austria, to written parliamentary questions by Stephanie Krisper, 7 October 2022, Reference 2022-0.575.143 https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12020/index.shtml

[1d] Response by Alma Zadić, Federal Minister of Justice, to written parliamentary questions by Stephanie Krisper, 7 October 2022, Reference 2022-0.575.216 https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12019/index.shtml

Or. en

Amendment 1188
Sophia in 't Veld

Motion for a resolution
Paragraph 166 a (new)

Motion for a resolution	*Amendment*
	166 a. In 2017, Finfisher's product FinSpy appeared in Turkey on a fake version of a mobilization website for the Turkish opposition. The software was disguised as a downloadable app recommended to participants in anti-government demonstrations[1a]. Finfisher itself advertised its products as solely fighting crime. In 2019, a criminal complaint was filed against Finfisher by Gesellschaft für Freiheitsrechte (GFF), Reporter ohne Grenzen (RSF Germany), the blog netzpolitik.org and the European Center for Constitutional and Human Rights (ECCHR), for exporting its spyware without the necessary export license from the German Federal Office for Economic Affairs and Export Control. It thereby violated the EU Dual-Use

Regulation and corresponding German national law. Following the complaint, the Public Prosecutor's Office of Munich investigated FinFisher, and in October 2020 it searched 15 business premises of the FinFisher group of companies in Germany and Romania and private residences. In 2021, the Munich District Court approved the seizure by the Public Prosecutor's Office's of Finfisher's bank accounts, in order to ensure confiscation of illegally obtained profits after FinFisher's possible conviction. However, FinFisher declared insolvency in February 2022. Business operations have ceased, the office has been closed, and all 22 employees were dismissed[1b]. The criminal investigations into the people responsible for FinFisher's activities are still ongoing.

[1a] ***https://www.ecchr.eu/en/case/surveillance-software-germany-turkey-finfisher/***

[1b] ***https://netzpolitik.org/2022/nach-pfaendung-staatstrojaner-hersteller-finfisher-ist-geschlossen-und-bleibt-es-auch/ https://edri.org/our-work/criminal-complaint-against-illegal-export-of-surveillance-software-is-making-an-impact-the-finfisher-group-of-companies-ceases-business-operations-after-its-accounts-are-seized-by-public-prosecutor/ https://netzpolitik.org/wp-upload/2022/03/2022-02-08_AG-Muenchen_Insolvenzbekanntmachung_FinFisher-Labs-GmbH.txt***

Or. en

Amendment 1189
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 166 a (new)

Motion for a resolution	*Amendment*
	166 a. In 2017, Finfisher's product FinSpy appeared in Turkey on a fake version of a mobilization website for the Turkish opposition. The software was disguised as a downloadable app recommended to participants in anti-government demonstrations. Finfisher itself advertised its products as solely fighting crime. In 2019, a criminal complaint was filed against Finfisher by Gesellschaft für Freiheitsrechte (GFF), Reporter ohne Grenzen (RSF Germany), the blog netzpolitik.org and the European Center for Constitutional and Human Rights (ECCHR), for exporting its spyware without the necessary export license from the German Federal Office for Economic Affairs and Export Control. It thereby violated the EU Dual-Use Regulation and corresponding German national law. Following the complaint, the Public Prosecutor's Office of Munich investigated FinFisher, and in October 2020 it searched 15 business premises of the FinFisher group of companies in Germany and Romania and private residences. In 2021, the Munich District Court approved the seizure by the Public Prosecutor's Office's of Finfisher's bank accounts, in order to ensure confiscation of illegally obtained profits after FinFisher's possible conviction. However, FinFisher declared insolvency in February 2022. Business operations have ceased, the office has been closed, and all 22 employees were dismissed. The criminal investigations into the people responsible for FinFisher's activities are still ongoing.

Or. en

Amendment 1190
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield,

Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 166 b (new)

Motion for a resolution	*Amendment*
	166 b. In 2011, Ahmed Mansoor, a human rights defender in the United Arab Emirates, was targeted with FinFisher's FinSpy spyware[330a]. FinFisher helped Bahrain install spyware on 77 computers, including those belonging to human rights lawyers and a subsequently jailed opposition leader, between 2010 and 2012—a period that includes Bahrain's crackdown on pro-democracy protesters[330b]. In 2012, FinFisher's software enabled the surveillance of Ethiopian political refugee Tadesse Kersmo by the Ethiopian government after he fled into EU exile, thereby heavily infringing upon the safe space that the EU claims to provide to persons at risk[330c].

[330a] CitizenLab: The Million Dollar Dissident. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

[330b] Amnesty International: A brief history of governments hacking human rights organizations. https://www.amnesty.org/en/latest/campaigns/2016/01/brief-history-of-government-hacking-human-rights-organizations/

[330c] Privacy International:Surveillance follows Ethiopian political refugee to the UK. https://privacyinternational.org/blog/1199/surveillance-follows-ethiopian-political-refugee-uk

Or. en

Amendment 1191
Gilles Lebreton, Christine Anderson, Mathilde Androuët

Motion for a resolution
Paragraph 167

Motion for a resolution	*Amendment*
167. ***Governments have targeted EU citizens with powerful spyware. This poses threats to democracy and individual citizens' rights. The EU has powers to act on these threats, albeit very few. When Member States, however, invoke 'national security', the EU is basically out of the game.*** Member States define national security unilaterally***, and can shut the door at any time. In addition to these legal constraints, there are political reasons that amount to EU-passiveness***. The European Commission, as guardian of the EU treaties, ***has grown reticent when it comes to enforcing EU law[331]. This is not because there are legal constraints, but rather because it is a political choice. The Commission tends to interpret its powers in the narrowest possible way. When faced with flagrant violations of the rule of law and fundamental rights, this stance becomes very problematic.*** Subsidiarity and respect for the exclusive national competences ***risks turning in to impunity. Below we will examine the powers that the EU institutions have at their disposal. The Parliament, Commission and Council have the power and the duty to legislate, regulate and enforce and they have to do so with vigour and ambition, putting defence of our democracy over short-term political considerations***.	167. Member States define national security unilaterally. The European Commission, as guardian of the EU treaties, ***is bound by*** subsidiarity and respect for the exclusive national competences.

331

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3994918

Or. fr

Amendment 1192
Dominik Tarczyński, Beata Kempa, Elżbieta Kruk
on behalf of the ECR Group

Motion for a resolution
Paragraph 167

Motion for a resolution	*Amendment*
167. ***Governments have targeted EU citizens with powerful*** spyware***. This*** poses threats to democracy and individual citizens' rights. The EU has powers to act on these threats, albeit very few. ***When Member States, however, invoke 'national security', the EU is basically out of the game. Member States define*** national security ***unilaterally, and can shut the door at any time.*** In addition to these legal constraints, there are political reasons that amount to EU-passiveness. The European ***Commission***, ***as guardian of*** the EU ***treaties, has grown reticent when it comes to enforcing EU law***[331] ***. This is not because there are legal constraints, but rather because it is a political choice. The Commission tends to interpret its powers in the narrowest possible way. When faced with flagrant violations of the rule of law and fundamental rights, this stance becomes very problematic. Subsidiarity and respect for the exclusive national competences risks turning in to impunity***. Below we will examine the powers that the EU institutions have at their disposal. ***The Parliament, Commission and Council have the power and the duty to legislate, regulate and enforce and they have to do so with vigour and ambition, putting defence of our democracy over short-term political considerations.***	167. ***The misuse of*** spyware poses threats to democracy and individual citizens' rights. The EU has powers to act on these threats, albeit very few. ***It should be recalled that, according to the Treaties, matters of*** national security ***remain the exclusive competence of the Member States. However*** in addition to these legal constraints, there are political reasons that amount to EU-passiveness. The ***source of this passivity is submission and servility towards the largest*** European ***countries***, ***while demonstrating strength towards the weakest countries. As a result, alleged abuses in weaker countries are publicized and exaggerated, while the biggest players remain completely beyond the reach of any disciplinary action by*** the EU. Below we will examine the powers that the EU institutions have at their disposal.

331 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3994918

Or. en

Amendment 1193
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Lucia Vuolo, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 167

Motion for a resolution	*Amendment*
167. Governments have targeted EU citizens with powerful spyware. This poses threats to democracy and ***individual*** citizens***' rights***. The EU ***has powers*** to act on these threats***, albeit very few. When Member States***, however, ***invoke 'national security', the EU is basically out of the game. Member States define*** national security ***unilaterally, and can shut the door at any time. In addition to these legal constraints, there are political reasons that amount to EU-passiveness. The European Commission, as guardian of the EU treaties, has grown reticent when it comes to enforcing*** EU law[331] ***. This is not because there are legal constraints, but rather because it is a political choice. The Commission tends to interpret its powers in the narrowest possible way. When faced with flagrant violations of the rule of law and*** fundamental rights***, this stance becomes very problematic. Subsidiarity and respect for the exclusive national competences risks turning in to impunity***. Below we will examine the powers that the EU institutions have at their disposal. The Parliament, Commission and Council have the power and the duty to legislate, regulate and enforce and they have to do so with vigour and ambition***, putting defence of our democracy over short-term political considerations***.	167. ***Some EU*** governments have targeted EU citizens with powerful spyware***, abusing their right to resort to surveillance in case of risk to national security***. This poses threats to democracy and ***fundamental rights of EU*** citizens. The EU ***should act within the scope of its competences*** to act on these threats***. One challenge***, however, ***stems from the ambiguity related to*** national security***, which under*** EU law ***remains exclusive competence of Member States and the necessity to reconcile this principle with*** fundamental rights ***and democratic norms strongly embedded in EU law***. Below we will examine the powers that the EU institutions have at their disposal. The Parliament, Commission and Council have the power and the duty to legislate, regulate and enforce and they have to do so with vigour and ambition ***to protect and implement European interests, norms and values***.

331 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3994918

Or. en

Amendment 1194
Carles Puigdemont i Casamajó

Motion for a resolution
Paragraph 167

Motion for a resolution	*Amendment*
167. Governments have targeted EU citizens with powerful spyware. This poses threats to democracy and individual citizens' rights. The EU has powers to act on these threats, albeit very few. When Member States, however, invoke 'national security', the EU is basically out of the game. Member States define national security unilaterally, and can shut the door at any time. In addition to these legal constraints, there are political reasons that amount to EU-passiveness. The European Commission, as guardian of the EU treaties, has grown reticent when it comes to enforcing EU law[331] . This is not because there are legal constraints, but rather because it is a political choice. The Commission tends to interpret its powers in the narrowest possible way. When faced with flagrant violations of the rule of law and fundamental rights, this stance becomes very problematic. Subsidiarity and respect for the exclusive national competences risks turning in to impunity. Below we will examine the powers that the EU institutions have at their disposal. The Parliament, Commission and Council have the power and the duty to legislate, regulate and enforce and they have to do so with vigour and ambition, putting defence of our democracy over short-term political considerations.	167. Governments have targeted EU citizens with powerful spyware. This poses threats to democracy and individual citizens' rights. The EU has powers to act on these threats, albeit very few. When Member States, however, invoke 'national security', the EU is basically out of the game. Member States define national security unilaterally, and can shut the door at any time. In addition to these legal constraints, there are political reasons that amount to EU-passiveness. The European Commission, as guardian of the EU treaties, has grown reticent when it comes to enforcing EU law[331] . This is not because there are legal constraints, but rather because it is a political choice. The Commission tends to interpret its powers in the narrowest possible way. When faced with flagrant violations of the rule of law and fundamental rights, this stance becomes very problematic. Subsidiarity and respect for the exclusive national competences risks turning in to impunity. Below we will examine the powers that the EU institutions have at their disposal. The Parliament, Commission and Council have the power and the duty to legislate, regulate and enforce and they have to do so with vigour and ambition, putting defence of our democracy over short-term political considerations. ***Programs like Pegasus, which structurally violate fundamental rights through the lack of control on its use, should be banned from the EU, and the Commission should make a legislative proposal to achieve such a goal.***
331	331

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3994918

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3994918

Or. en

Amendment 1195
Sophia in 't Veld

Motion for a resolution
Paragraph 167

Motion for a resolution	*Amendment*
167. Governments have targeted EU citizens with powerful spyware. This poses threats to democracy and individual citizens' rights. The EU has powers to act on these threats, albeit very few. When Member States, however, invoke 'national security', the EU is basically out of the game. Member States define national security unilaterally, and can shut the door at any time. In addition to these legal constraints, there are political reasons that amount to EU-passiveness. The European Commission, as guardian of the EU treaties, has grown reticent when it comes to enforcing EU law[331] . This is not because there are legal constraints, but rather because it is a political choice. The Commission ***tends*** to interpret its powers in the narrowest possible way. When faced with flagrant violations of the rule of law and fundamental rights, this ***stance*** becomes very problematic. Subsidiarity and respect for the exclusive national competences risks turning in to impunity. Below we will examine the powers that the EU institutions have at their disposal. The Parliament, Commission and Council have the power and the duty to legislate, regulate and enforce and they have to do so with vigour and ambition, putting defence of our democracy over short-term political considerations.	167. Governments have targeted EU citizens with powerful spyware. This poses threats to democracy and individual citizens' rights. The EU has powers to act on these threats, albeit very few. When Member States, however, invoke 'national security', the EU is basically out of the game. Member States define national security unilaterally, and can shut the door at any time. In ***this way, Member States are escaping transparency and accountability, and allow for umhampered use, and trade in spyware. In*** addition to these legal constraints, there are political reasons that amount to EU-passiveness. The European Commission, as guardian of the EU treaties, has grown reticent when it comes to enforcing EU law[331] . This is not because there are legal constraints, but rather because it is a political choice. The Commission ***is stonewalling the matter, and chooses*** to interpret its powers in the narrowest possible way. When faced with flagrant violations of the rule of law and fundamental rights, this ***policy of forbearance*** becomes very problematic. Subsidiarity and respect for the exclusive national competences risks turning in to impunity. Below we will examine the powers that the EU institutions have at their disposal. The Parliament, Commission and Council have the power and the duty to legislate, regulate and enforce and they have to do so with vigour

and ambition, putting defence of our democracy over short-term political considerations.

331 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3994918

331 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3994918

Or. en

Amendment 1196
Cornelia Ernst, Stelios Kouloglou, Giorgos Georgiou, Anne-Sophie Pelletier

Motion for a resolution
Paragraph 167

Motion for a resolution	*Amendment*
167. Governments have targeted EU citizens with powerful spyware. This poses threats to democracy and individual citizens' rights. The EU has powers to act on these threats, albeit very few. When Member States, however, invoke 'national security', the EU is basically out of the game. Member States define national security unilaterally, and can shut the door at any time. In addition to these legal constraints, there are political reasons that amount to EU-passiveness. The European Commission, as guardian of the EU treaties, has grown reticent when it comes to enforcing EU law[331] . This is not because there are legal constraints, but rather because it is a political choice. The Commission tends to interpret its powers in the narrowest possible way. When faced with flagrant violations of the rule of law and fundamental rights, this stance becomes very problematic. Subsidiarity and respect for the exclusive national competences risks turning in to impunity. Below we will examine the powers that the EU institutions have at their disposal. The Parliament, Commission and Council have the power and the duty to legislate, regulate and enforce and they have to do so	167. Governments have targeted EU citizens with powerful ***and highly invasive*** spyware. This poses threats to democracy ***fundamental rights, rule of law*** and individual citizens' rights. The EU has powers to act on these threats, albeit very few. When Member States, however, invoke 'national security', the EU is basically out of the game. Member States define national security unilaterally, and can shut the door at any time. In addition to these legal constraints, there are political reasons that amount to EU-passiveness. The European Commission, as guardian of the EU treaties, has grown reticent when it comes to enforcing EU law[331] . This is not because there are legal constraints, but rather because it is a political choice. The Commission tends to interpret its powers in the narrowest possible way. When faced with flagrant violations of the rule of law and fundamental rights, this stance becomes very problematic. Subsidiarity and respect for the exclusive national competences risks turning in to impunity. Below we will examine the powers that the EU institutions have at their disposal. The Parliament, Commission and Council have the power and the duty to legislate,

with vigour and ambition, putting defence of our democracy over short-term political considerations.

regulate and enforce and they have to do so with vigour and ambition, putting defence of our democracy over short-term political considerations.

331 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3994918

331 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3994918

Or. en

Amendment 1197
Ivo Hristov

Motion for a resolution
Paragraph 167 a (new)

Motion for a resolution	*Amendment*
	167 a. In order to respond to the spread and use of spyware technologies in the Union's territory that have a negative effect on the respect of basic human rights, such as the right of privacy, the EU could set up an operational entity capable of inspecting potentially infected devices to ensure the protection of European citizens.

Or. en

Amendment 1198
Sophia in 't Veld

Motion for a resolution
Paragraph 168

Motion for a resolution	*Amendment*
168. The European Commission, in its response to the spyware scandal, has so far limited itself to writing letters requesting clarification from the governments of Poland, Hungary, Spain and Greece. However, ***it would seem that*** this timid	168. The European Commission, in its response to the spyware scandal, has so far limited itself to writing letters requesting clarification from the governments of Poland, Hungary, Spain and Greece. However, this timid admonition by the

admonition by the Commission ***will not be*** followed by further action. It is true that strictly speaking the Commission has no powers to act in the area of national security. However, as the Commission itself points out in those letters, 'national security' should not be interpreted as an unlimited carve out from European laws and Treaties, and become an area of lawlessness.

Commission ***has not been*** followed by further action. It is true that strictly speaking the Commission has no powers to act in the area of national security. However, as the Commission itself points out in those letters, 'national security' should not be interpreted as an unlimited carve out from European laws and Treaties, and become an area of lawlessness. ***It is up to the Member States however to "demonstrate that national security would be compromised in the case at issue." In response to the question what actions the Commission will take if national authorities do not thoroughly examine any allegations of illegal spying, the Commission merely refers to the European Court of Justice and to Article 47 of the Charter, which grants a right to an effective remedy before a tribunal. There seems to be no political willingness to act.***

Or. en

Amendment 1199
Gilles Lebreton, Christine Anderson, Mathilde Androuët

Motion for a resolution
Paragraph 168

Motion for a resolution	*Amendment*
168. The European Commission, in its response to the spyware scandal, has ***so far limited itself to writing*** letters requesting clarification from the governments of Poland, Hungary, Spain and Greece. ***However,*** it would seem that this ***timid admonition by the Commission will not be*** followed by further action. It is true that strictly speaking the Commission has no powers to act in the area of national security. ***However, as the Commission itself points out in those letters, 'national security' should not be interpreted as an unlimited carve out from European laws and Treaties, and become an area of***	168. The European Commission, in its response to the spyware scandal, has ***written*** letters requesting clarification from the governments of Poland, Hungary, Spain and Greece. It would seem that this ***is not being*** followed by further action. It is true that strictly speaking the Commission has no powers to act in the area of national security.

lawlessness.

Or. fr

Amendment 1200
Dominik Tarczyński, Beata Kempa, Elżbieta Kruk
on behalf of the ECR Group

Motion for a resolution
Paragraph 168

Motion for a resolution	*Amendment*
168. The European Commission, in its response to the spyware scandal, has so far limited itself to writing letters requesting clarification from the governments of Poland, Hungary, Spain and Greece. However, it would seem that this timid admonition by the Commission will not be followed by further action. It is true that strictly speaking the Commission has no powers to act in the area of national security. ***However, as the Commission itself points out in those letters, 'national security' should not be interpreted as an unlimited carve out from European laws and Treaties, and become an area of lawlessness.***	168. The European Commission, in its response to the spyware scandal, has so far limited itself to writing letters requesting clarification from the governments of Poland, Hungary, Spain and Greece. However, it would seem that this timid admonition by the Commission will not be followed by further action. It is true that strictly speaking the Commission has no powers to act in the area of national security.

Or. en

Amendment 1201
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Lucia Vuolo, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 168

Motion for a resolution	*Amendment*
168. The European Commission, in its response to the spyware scandal, has so far ***limited itself to writing letters*** requesting clarification from the governments of Poland, Hungary, Spain and Greece***.***	168. The European Commission***, has no powers to act in the area of national security. Thus***, in its response to the spyware scandal, ***it*** has so far ***taken only few steps, which included*** requesting

However, it would seem that this timid admonition by the Commission ***will not be followed by further action. It is true that strictly speaking the Commission has no powers to act in the area of national security. However, as the Commission itself points out in those letters, 'national security' should not be interpreted as an unlimited carve out from European laws and Treaties, and become an area of lawlessness.***

clarification from the governments of Poland, Hungary, Spain and Greece***, launching inquiry into reported attempts to hack EU Commissioners and members of*** Commission ***staff, devoting more attention to reports of abuse of spyware in annual rule of law reports***.

Or. en

Amendment 1202
Carles Puigdemont i Casamajó

Motion for a resolution
Paragraph 168

Motion for a resolution	*Amendment*
168. The European Commission, in its response to the spyware scandal, has so far limited itself to writing letters requesting clarification from the governments of Poland, Hungary, Spain and Greece. However, it would seem that this timid admonition by the Commission will not be followed by further action. It is true that strictly speaking the Commission has no powers to act in the area of national security. However, as the Commission itself points out in those letters, 'national security' should not be interpreted as an unlimited carve out from European laws and Treaties, and become an area of lawlessness.	168. The European Commission, in its response to the spyware scandal, has so far limited itself to writing letters requesting clarification from the governments of Poland, Hungary, Spain and Greece. However, it would seem that this timid admonition by the Commission will not be followed by further action. It is true that strictly speaking the Commission has no powers to act in the area of national security. However, as the Commission itself points out in those letters, 'national security' should not be interpreted as an unlimited carve out from European laws and Treaties, and become an area of lawlessness***, but it does have powers over the defence of the rule of law in the European Union***.

Or. en

Amendment 1203
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Lucia Vuolo, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 168 a (new)

Motion for a resolution	*Amendment*
	168 a. In addition, the Commission continues to monitor and enforce implementation of existing regulatory tools which can play a role in protecting rights of EU citizens against potential abuses of spyware, such as GDPR and e-Privacy and Law Enforcement Directive. It also monitors implementation of Dual-Use regulation.

Or. en

Amendment 1204
Carles Puigdemont i Casamajó

Motion for a resolution
Paragraph 168 a (new)

Motion for a resolution	*Amendment*
	168 a. Taking all this into account, the European Commission should thus open procedures on those countries where Pegasus has been used against political rivals, activists or journalists.

Or. en

Amendment 1205
Ivo Hristov

Motion for a resolution
Paragraph 168 a (new)

Motion for a resolution	*Amendment*
	168 a. The Commission may include the standards in national legislation in this field in its annual Rule of Law reports.

Or. en

Amendment 1206
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Lucia Vuolo, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 168 b (new)

Motion for a resolution	*Amendment*
	168 b. In a letter to the PEGA Committee, the Commission declared that it would support the development of new technologies to ensure internal security and cybersecurity for all.

Or. en

Amendment 1207
Sophia in 't Veld

Motion for a resolution
Paragraph 169

Motion for a resolution	*Amendment*
169. Unlike the US, the Commission has so far not undertaken an analysis of the situation nor an assessment of the companies that are active in the European market. There is no obvious legal objection against conducting such an analysis.	169. Unlike the US***, which is taking action with determination to tackle mercenary spyware, more than a year and a half after the first revelations***, the Commission has ***regrettably*** so far not ***even*** undertaken an analysis of the situation nor an assessment of the companies that are active in the European market. There is no obvious legal objection against conducting such an analysis. ***It is highly remarkable that the large amount of evidence published over the past year has still not incited the Commission to take any meaningful action. Although the Commission generally quickly condemns threats to the Union from third countries, it prefers to remain quiet when it comes to threats from Member States. The Commission knowlingly condones the***

violation of citizens' rights and the destruction of democracy. Its inertia amounts to complicity in human rights violations and delericiton of duty.

Or. en

Amendment 1208
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Lucia Vuolo, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 169

Motion for a resolution	*Amendment*
169. ***Unlike the US,*** the Commission has so far not undertaken an analysis of the situation nor an assessment of the companies that are active ***in the European*** market***. There is no obvious legal objection against conducting such an analysis***.	169. The Commission has so far not undertaken an analysis of the situation nor an assessment of the companies that are active ***on the spyware*** market ***within the EU***.

Or. en

Amendment 1209
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Lucia Vuolo, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 170

Motion for a resolution	*Amendment*
170. The EU does have several laws that might serve as regulatory tools with regard to spyware. In addition to laws protecting the rights of citizens, such as the laws on data protection and privacy of communications (GDPR, e-Privacy), there are laws on exports (Dual Use Regulation) and procurement. However, enforcement by the Commission is weak. It tends to limit itself to verifying if a Member State has correctly transposed	***deleted***

EU laws in national laws. However, that says very little about the actual situation on the ground. Thus, the Commission implementation report[332] of the Dual Use Regulation seems to conclude that implementation is well on track, whereas there is ample evidence to prove that in practice it is weak and patchy, and in some countries even deliberately so. Despite the rules laid down in the Dual Use Regulation, Cyprus appears to have become an attractive export hub for spyware vendors. Without proper and meaningful enforcement, EU laws are mere paper tigers that create ample space for the illegitimate use of spyware.

---

[332] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223

Or. en

Amendment 1210
Sophia in 't Veld

Motion for a resolution
Paragraph 170

Motion for a resolution	*Amendment*
170. The EU does have several laws that might serve as regulatory tools with regard to spyware. In addition to laws protecting the rights of citizens, such as the laws on data protection and privacy of communications (GDPR, e-Privacy), there are laws on exports (Dual Use Regulation) and procurement. However, enforcement by the Commission is weak. It tends to limit itself to verifying if a Member State has correctly transposed EU laws in national laws. However, that says very little about the actual situation on the ground. Thus, the Commission implementation report[332] of the Dual Use Regulation seems to conclude that	170. The EU does have several laws that might serve as regulatory tools with regard to spyware. In addition to laws protecting the rights of citizens, such as the laws on data protection and privacy of communications (GDPR, e-Privacy), there are laws on exports (Dual Use Regulation) and procurement. However, enforcement by the Commission is weak***. It does not exert its role as Guardian of the Treaties properly and in good faith***. It tends to limit itself to verifying if a Member State has correctly transposed EU laws in national laws. However, that says very little about the actual situation on the ground. Thus, the Commission implementation report[332]

implementation is well on track, whereas there is ample evidence to prove that in practice it is weak and patchy, and in some countries even deliberately so. Despite the rules laid down in the Dual Use Regulation, Cyprus appears to have become an attractive export hub for spyware vendors. Without proper and meaningful enforcement, EU laws are mere paper tigers that create ample space for the illegitimate use of spyware.	of the Dual Use Regulation seems to conclude that implementation is well on track, whereas there is ample evidence to prove that in practice it is weak and patchy, and in some countries even deliberately so. Despite the rules laid down in the Dual Use Regulation, Cyprus appears to have become an attractive export hub for spyware vendors. ***Also the implementation of the e-Privacy Directive and of judgments by the CJEU in relation to this law is very poor. The Commission refers to the Member States as responsible for implementation and enforcement of the Directive in compliance with CJEU jurisprudence, but does not take action when Member States fail to do so.*** Without proper and meaningful enforcement, EU laws are mere paper tigers that create ample space for the illegitimate use of spyware.
[332] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223	[332] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223
	Or. en

Amendment 1211
Ivo Hristov

Motion for a resolution
Paragraph 170

Motion for a resolution	*Amendment*
170. The EU does have several laws that might serve as regulatory tools with regard to spyware. In addition to laws protecting the rights of citizens***, such as the laws on data protection and privacy of communications (GDPR, e-Privacy)***, there are laws on exports (Dual Use Regulation) and procurement. However, enforcement by the Commission is weak. It tends to limit itself to verifying if a Member State has correctly transposed EU laws in	170. The EU does have several laws that might serve as regulatory tools with regard to spyware. ***However, the application of the Union's law to the use of spyware for national security purposes is largely limited due to the exclusion of national security from the scope of GDPR and ePrivacy Directive.*** In addition to laws protecting the rights of citizens, there are laws on exports (Dual Use Regulation) and procurement. However, enforcement by the

national laws. However, that says very little about the actual situation on the ground. Thus, the Commission implementation report[332] of the Dual Use Regulation seems to conclude that implementation is well on track, whereas there is ample evidence to prove that in practice it is weak and patchy, and in some countries even deliberately so. Despite the rules laid down in the Dual Use Regulation, Cyprus appears to have become an attractive export hub for spyware vendors. Without proper and meaningful enforcement, EU laws are mere paper tigers that create ample space for the illegitimate use of spyware.

[332] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223

Commission is weak. It tends to limit itself to verifying if a Member State has correctly transposed EU laws in national laws. However, that says very little about the actual situation on the ground***. There is need to strenghten protection in order to guarantee that cyber survelliance items would not be exported to coutries that do not respect fundamental rights and equal attention should be paid to imports as well***. Thus, the Commission implementation report[332] of the Dual Use Regulation seems to conclude that implementation is well on track, whereas there is ample evidence to prove that in practice it is weak and patchy, and in some countries even deliberately so. Despite the rules laid down in the Dual Use Regulation, Cyprus appears to have become an attractive export hub for spyware vendors. Without proper and meaningful enforcement ***that goes beyond blacklisting of spyware vendors***, EU laws are mere paper tigers that create ample space for the illegitimate use of spyware.

[332] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223

Or. en

Amendment 1212
Gilles Lebreton, Christine Anderson, Mathilde Androuët

Motion for a resolution
Paragraph 170

Motion for a resolution	*Amendment*
170. The EU does have several laws that might serve as regulatory tools with regard to spyware. In addition to laws protecting the rights of citizens, such as the laws on data protection and privacy of communications (GDPR, e-Privacy), there are laws on exports (Dual Use Regulation)	170. The EU does have several laws that might serve as regulatory tools with regard to spyware. In addition to laws protecting the rights of citizens, such as the laws on data protection and privacy of communications (GDPR, e-Privacy), there are laws on exports (Dual Use Regulation)

and procurement. ***However,*** enforcement by the Commission ***is weak. It*** tends to limit itself to verifying if a Member State has correctly transposed EU laws in national laws. However, ***that says very little about the actual situation on the ground. Thus, the Commission implementation report[332]of the Dual Use Regulation seems to conclude that implementation is well on track, whereas there is ample evidence to prove that in practice it is weak and patchy, and in some countries even deliberately so. Despite the rules laid down in the Dual Use Regulation, Cyprus appears to have become an attractive export hub for spyware vendors.*** Without proper and meaningful enforcement, EU laws are mere paper tigers that create ample space for the illegitimate use of spyware.	and procurement. Enforcement by the Commission tends to limit itself to verifying if a Member State has correctly transposed EU laws in national laws. However, without proper and meaningful enforcement, EU laws are mere paper tigers that create ample space for the illegitimate use of spyware.

[332] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223

Or. fr

Amendment 1213
Dominik Tarczyński, Beata Kempa, Elżbieta Kruk
on behalf of the ECR Group

Motion for a resolution
Paragraph 170

Motion for a resolution	*Amendment*
170. The EU does have several laws that might serve as regulatory tools with regard to spyware. In addition to laws protecting the rights of citizens, such as the laws on data protection and privacy of communications (GDPR, e-Privacy), there are laws on exports (Dual Use Regulation) and procurement. However, enforcement by the Commission is weak. It tends to limit itself to verifying if a Member State has correctly transposed EU laws in	170. The EU does have several laws that might serve as regulatory tools with regard to spyware. In addition to laws protecting the rights of citizens, such as the laws on data protection and privacy of communications (GDPR, e-Privacy), there are laws on exports (Dual Use Regulation) and procurement. However, enforcement by the Commission is weak. It tends to limit itself to verifying if a Member State has correctly transposed EU laws in

national laws. However, that says very little about the actual situation on the ground. Thus, the Commission implementation report[332] of the Dual Use Regulation seems to conclude that implementation is well on track, whereas there is ample evidence to prove that in practice it is weak and patchy, and in some countries even deliberately so. Despite the rules laid down in the Dual Use Regulation, Cyprus appears to have become an attractive export hub for spyware vendors. ***Without proper and meaningful enforcement, EU laws are mere paper tigers that create ample space for the illegitimate use of spyware.***

[332] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223

national laws. However, that says very little about the actual situation on the ground. Thus, the Commission implementation report[332] of the Dual Use Regulation seems to conclude that implementation is well on track, whereas there is ample evidence to prove that in practice it is weak and patchy, and in some countries even deliberately so. Despite the rules laid down in the Dual Use Regulation, Cyprus appears to have become an attractive export hub for spyware vendors.

[332] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223

Or. en

Amendment 1214
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Andrzej Halicki, Bartosz Arłukowicz, Radosław Sikorski, Lucia Vuolo, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 170 a (new)

Motion for a resolution	*Amendment*
	170 a. The Law Enforcement Directive was meant to provide high standards of data protection and ensure the free flow of data in the law enforcement and criminal justice sector. The Directive had to be transposed into national laws, with broad discretionary powers given to Member States. Today it is evident that implementation differs from Member State to Member State, especially in the area of data subject's rights. The European Commission should urgently assess the implementation in all Member States and identify the most serious

shortcomings. The Commission should develop concrete guidance to Member States on implementation in order to ensure that EU standards are respected across the Union. Furthermore, where necessary, the Commission should start infringement procedures in cases the Directive was not transposed correctly and there is lack of willingness from a Member States to correct it.

Or. en

Amendment 1215
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Lucia Vuolo, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 171

Motion for a resolution	*Amendment*
171. The European Parliament has set up the PEGA inquiry committee***, which is working diligently and effectively*** within its ***powers and*** mandate. ***However, it has no powers to summon witnesses or hear them under oath, and it has no access to classified information. It lacks the full investigative powers that most national parliaments have. In addition, the influence of national governments is frequently present in the deliberations of PEGA, which on occasion is an obstacle to thorough, fully independent, and objective investigations. It is quite cynical that the European Parliament does not have the full powers to investigate, when some of its own members are victims of illegal surveillance.***	171. The European Parliament has set up the PEGA inquiry committee ***acting*** within ***the scope of*** its mandate.

Or. en

Amendment 1216
Gilles Lebreton, Christine Anderson, Mathilde Androuët

Motion for a resolution
Paragraph 171

Motion for a resolution	*Amendment*
171. The European Parliament has set up the PEGA inquiry committee, which is working diligently and effectively within its powers and mandate. However, it has no powers to summon witnesses or hear them under oath, and it has no access to classified information. It lacks the full investigative powers that most national parliaments have. ***In addition, the influence of national governments is frequently present in the deliberations of PEGA, which on occasion is an obstacle to thorough, fully independent, and objective investigations. It is quite cynical that the European Parliament does not have the full powers to investigate, when some of its own members are victims of illegal surveillance.***	171. The European Parliament has set up the PEGA inquiry committee, which is working diligently and effectively within its powers and mandate. However, it has no powers to summon witnesses or hear them under oath, and it has no access to classified information. It lacks the full investigative powers that most national parliaments have.

Or. fr

Amendment 1217
Dominik Tarczyński, Beata Kempa, Elżbieta Kruk
on behalf of the ECR Group

Motion for a resolution
Paragraph 171

Motion for a resolution	*Amendment*
171. The European Parliament has set up the PEGA inquiry committee, which is working ***diligently and effectively*** within its powers and mandate. However, it has no powers to summon witnesses or hear them under oath, and it has no access to classified information. ***It lacks the full investigative powers that most national parliaments have.*** In addition, the influence of national governments is frequently present in the deliberations of PEGA***,*** which on occasion is an obstacle to thorough, fully independent, and objective	171. The European Parliament has set up the PEGA inquiry committee, which is working within its powers and mandate. However, it has no powers to summon witnesses or hear them under oath, and it has no access to classified information. In addition, the influence of national governments is frequently present in the deliberations of PEGA ***- and manifests itself primarily in the unequal treatment of EU countries and channeling the investigation only around countries disliked in the EU -*** which on occasion is

investigations. ***It is quite cynical that the European Parliament does not have the full powers to investigate, when some of its own members are victims of illegal surveillance.***	an obstacle to thorough, fully independent, and objective investigations.

Or. en

Amendment 1218
Sophia in 't Veld

Motion for a resolution
Paragraph 171

Motion for a resolution	*Amendment*
171. The European Parliament has set up the PEGA inquiry committee, which ***is*** working diligently and effectively within its powers and mandate. However, it has no powers to summon witnesses or hear them under oath, and it has no access to classified information. It lacks the full investigative powers that most national parliaments have. In addition, the influence of national governments is frequently present in the deliberations of PEGA, which on occasion is an obstacle to thorough, fully independent, and objective investigations. It is quite cynical that the European Parliament does not have the full powers to investigate, when some of its own members are victims of illegal surveillance.	171. The European Parliament has set up the PEGA inquiry committee, which ***has been*** working diligently and effectively within its powers and mandate. However, it has no powers to summon witnesses or hear them under oath, and it has no access to classified information. It lacks the full investigative powers that most national parliaments have. In addition, the influence of national governments is frequently present in the deliberations of PEGA, which on occasion is an obstacle to thorough, fully independent, and objective investigations. It is quite cynical that the European Parliament does not have the full powers to investigate, when some of its own members are victims of illegal surveillance.

Or. en

Amendment 1219
Ivo Hristov

Motion for a resolution
Paragraph 171 a (new)

Motion for a resolution	*Amendment*
	171 a. The EP may support a dedicated

	initiative to monitor surveillance equipment imports and exports from the EU in the light of a global spread of surveillance equipment.

Or. en

Amendment 1220
Dominik Tarczyński, Beata Kempa, Elżbieta Kruk
on behalf of the ECR Group

Motion for a resolution
Subheading 127

Motion for a resolution	*Amendment*
European Council and Council of Ministers	***deleted***

Or. en

Amendment 1221
Gilles Lebreton, Christine Anderson, Mathilde Androuët

Motion for a resolution
Paragraph 172

Motion for a resolution	*Amendment*
172. Although the national governments claim that the spyware scandal is a purely national matter, it was actually discussed in the Council of the European Union and the national governments decided to respond collectively to the questionnaire of the European Parliament[333]. In doing so, they have fully acknowledged that it is in fact a matter for the Council. However, responsibility is not a menu that you can pick and choose from: you cannot only selectively deal with procedural matters, but not the substance.	***deleted***

[333] Draft letter from General Secretariat

of the Council to the Delegations, 26 September 2022.

Or. fr

Amendment 1222
Dominik Tarczyński, Beata Kempa, Elżbieta Kruk
on behalf of the ECR Group

Motion for a resolution
Paragraph 172

Motion for a resolution	*Amendment*
172. Although the national governments claim that the spyware scandal is a purely national matter, it was actually discussed in the Council of the European Union and the national governments decided to respond collectively to the questionnaire of the European Parliament[333] . In doing so, they have fully acknowledged that it is in fact a matter for the Council. However, responsibility is not a menu that you can pick and choose from: you cannot only selectively deal with procedural matters, but not the substance.	***deleted***

[333] Draft letter from General Secretariat of the Council to the Delegations, 26 September 2022.

Or. en

Amendment 1223
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 172

Motion for a resolution	*Amendment*
172. Although the national	***deleted***

governments claim that the spyware scandal is a purely national matter, it was actually discussed in the Council of the European Union and the national governments decided to respond collectively to the questionnaire of the European Parliament[333] . In doing so, they have fully acknowledged that it is in fact a matter for the Council. However, responsibility is not a menu that you can pick and choose from: you cannot only selectively deal with procedural matters, but not the substance.

---

*[333] **Draft letter from General Secretariat of the Council to the Delegations, 26 September 2022.***

Or. en

Amendment 1224
Sophia in 't Veld

Motion for a resolution
Paragraph 172

Motion for a resolution	*Amendment*
172. Although the national governments claim that the spyware scandal is a purely national matter, it was actually discussed in the Council of the European Union and the national governments decided to respond collectively to the questionnaire of the European Parliament[333] . In doing so, they have fully acknowledged that it is in fact a matter for the Council. However, responsibility is not a menu that you can pick and choose from: you cannot only selectively deal with procedural matters, but not the substance.	172. Although the national governments claim that the spyware scandal is a purely national matter, it was actually discussed in the Council of the European Union and the national governments decided to respond collectively to the questionnaire of the European Parliament[333] . In doing so, they have fully acknowledged that it is in fact a matter for the Council. However, responsibility is not a menu that you can pick and choose from: you cannot only selectively deal with procedural matters, but not the substance. ***The omertà and lack of cooperation of the Council does not bode well for any future regulatory initiatives. The Council is a legislator, but it may well be reluctant to regulate its own members.***

[333] Draft letter from General Secretariat of the Council to the Delegations, 26 September 2022.

[333] Draft letter from General Secretariat of the Council to the Delegations, 26 September 2022.

Or. en

Amendment 1225
Dominik Tarczyński, Beata Kempa, Elżbieta Kruk
on behalf of the ECR Group

Motion for a resolution
Paragraph 173

Motion for a resolution	*Amendment*
173. To date, the European Council has not responded publicly or substantively to the scandal. Some of its members have a stake in the matter, as they themselves may be complicit in the illegitimate hacks, or they simply wish to keep the EU weak and powerless in this area. The omertà and lack of cooperation of the Council does not bode well for any future regulatory initiatives. The Council is a legislator, but it may well be reluctant to regulate its own members.	***deleted***

Or. en

Amendment 1226
Gilles Lebreton, Christine Anderson, Mathilde Androuët

Motion for a resolution
Paragraph 173

Motion for a resolution	*Amendment*
173. To date, the European Council has not responded publicly or substantively to the scandal. ***Some of its members have a stake in the matter, as they themselves may be complicit in the illegitimate hacks, or they simply wish to keep the EU weak and powerless in this area. The omertà***	173. To date, the European Council has not responded publicly or substantively to the scandal.

and lack of cooperation of the Council does not bode well for any future regulatory initiatives. The Council is a legislator, but it may well be reluctant to regulate its own members.

Or. fr

Amendment 1227
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 173

Motion for a resolution	*Amendment*
173. To date, the European Council has not responded publicly or substantively to the scandal. ***Some of its members have a stake in the matter, as they themselves may be complicit in the illegitimate hacks, or they simply wish to keep the EU weak and powerless in this area. The omertà and lack of cooperation of*** the Council ***does not bode well for any future regulatory initiatives. The Council is a legislator, but it may well be reluctant to regulate its own members***.	173. To date, the European Council has not responded publicly or substantively to the scandal. ***The issue was discussed in*** the Council ***of the EU and the decision to respond collectively to the questionnaire of the European Parliament was made***.

Or. en

Amendment 1228
Sophia in 't Veld

Motion for a resolution
Paragraph 173

Motion for a resolution	*Amendment*
173. To date, the European Council has not responded publicly or substantively to the scandal. Some of its members have a stake in the matter, as they themselves may be complicit in the illegitimate hacks, or they simply wish to keep the EU weak and	173. To date, the European Council has not responded publicly or substantively to the scandal. Some of its members have a stake in the matter, as they themselves may be complicit in the illegitimate hacks, or they simply wish to keep the EU weak and

powerless in this area. ***The omertà and lack of cooperation of the Council does not bode well for any future regulatory initiatives. The Council is a legislator, but it may well be reluctant to regulate its own members.***	powerless in this area.

Or. en

Amendment 1229
Carles Puigdemont i Casamajó

Motion for a resolution
Paragraph 173

Motion for a resolution	*Amendment*
173. To date, the European Council has not responded publicly or substantively to the scandal. Some of its members have a stake in the matter, as they themselves may be complicit in the illegitimate hacks, or they simply wish to keep the EU weak and powerless in this area. The omertà and lack of cooperation of the Council does not bode well for any future regulatory initiatives***. The Council is a legislator, but it may well be reluctant to regulate its own members***.	173. To date, the European Council has not responded publicly or substantively to the scandal. Some of its members have a stake in the matter, as they themselves may be complicit in the illegitimate hacks, or they simply wish to keep the EU weak and powerless in this area. The omertà***, the unanimity rule*** and lack of cooperation of the Council does not bode well for any future regulatory initiatives ***and calls for an extra effort by the European Commission to ensure that Member States do not violate fundamental rights and to take measures when they do, as it already happened***.

Or. en

Amendment 1230
Dominik Tarczyński, Beata Kempa, Elżbieta Kruk
on behalf of the ECR Group

Motion for a resolution
Paragraph 174

Motion for a resolution	*Amendment*
174. Even if illegal or criminal behaviour was ultimately to be proven,	***deleted***

members of national governments cannot be impeached or made to resign from their EU jobs. This means that persons who are guilty of such acts may well continue with impunity to sit on EU bodies and take decisions affecting all European citizens.

Or. en

Amendment 1231
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 174

Motion for a resolution	*Amendment*
174. ***Even if illegal or criminal behaviour was ultimately to be proven,*** members of national governments cannot be impeached or made to resign from their EU jobs***. This means that persons who are guilty of such acts may well continue with impunity to sit on EU bodies and take decisions affecting all European citizens***.	174. Members of national governments cannot be impeached or made to resign from their EU jobs ***as it is the responsibility of individual Member States***.

Or. en

Amendment 1232
Carles Puigdemont i Casamajó

Motion for a resolution
Paragraph 174

Motion for a resolution	*Amendment*
174. ***Even if illegal or criminal behaviour was ultimately to be proven,*** members of national governments ***cannot be impeached or made to*** resign from their ***EU jobs. This means that persons*** who are guilty of such acts ***may well*** continue with impunity to sit on EU bodies and take decisions affecting all European citizens.	174. Members of national governments ***responsible for these violations of fundamental rights should*** resign from their ***posts. Those*** who are guilty of such acts ***should not*** continue with impunity to sit on EU bodies and take decisions affecting all European citizens. ***Moreover, they should not be invited to the European***

Parliament.

Or. en

Amendment 1233
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold, Andrzej Halicki, Bartosz Arłukowicz, Radosław Sikorski, Frances Fitzgerald

Motion for a resolution
Paragraph 174 a (new)

Motion for a resolution	*Amendment*
	174 a. Fighting serious crime and the ability to do so is a critically important aim for Member States. The protection of democracy and fundamental rights is also vital. The use of spyware by Member States must be proportionate to the crime committed, must not be arbitrary, and surveillance must only be authorised in narrowly, pre-determined circumstances. In this regard, a key priority should be the effective ex-ante mechanisms which ensure judicial oversight. This is essential to protect individual freedoms, particularly from authoritarian governments. Individual rights cannot be put at risk by unfettered access to surveillance. The ability of the judiciary to perform meaningful and effective ex-post oversight in the area of requests for surveillance for national security perspectives is also important, to ensure that disproportionate use of spyware by Governments can be challenged.

Or. en

Amendment 1234
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 175

Motion for a resolution	*Amendment*
175. Europol ***was requested to assist*** the Cypriot police and an academic expert in conducting a three-level forensic examination of the equipment found in the black van of Tal Dilian in 2019. During the PEGA hearing on 30 August 2022***,*** Europol ***made no reference to this, despite questions by Members on Europol's role in investigating spyware in the EU***. ***It has not been mentioned since.***	175. Europol ***provided support to*** the Cypriot police and an academic expert in conducting a three-level forensic examination of the equipment found in the black van of Tal Dilian in 2019. During the PEGA hearing on 30 August 2022 Europol ***explained the support provided by the Agency***.

Or. en

Amendment 1235
Cornelia Ernst, Stelios Kouloglou, Giorgos Georgiou, Anne-Sophie Pelletier

Motion for a resolution
Paragraph 176

Motion for a resolution	*Amendment*
176. Europol does not have any autonomous operational powers, and it cannot act without the consent and cooperation of the Member State(s) concerned. That presents a problem when there is clear evidence of criminal acts - such as cybercrime, corruption and extortion - but national authorities fail to investigate. This problem is made worse when the Member State authorities are themselves complicit in the crimes.	***deleted***

Or. en

Amendment 1236
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Lucia Vuolo, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 176

Motion for a resolution	*Amendment*
176. Europol does not have any autonomous operational powers, and it cannot act without the consent and cooperation of the Member State(s) concerned. ***That presents a problem when there is clear evidence*** of criminal ***acts - such as cybercrime, corruption and extortion - but*** national authorities ***fail to investigate***. ***This problem is made worse when the Member State authorities are themselves complicit in the crimes.***	176. Europol does not have any autonomous operational powers, and it cannot act without the consent and cooperation of the Member State(s) concerned. ***While Article 6 of the amended Europol Regulation determines that Europol may propose to the competent authorities of the Member State concerned the initiation, conduct or coordination*** of criminal ***investigations, Europol's competencies in the amended Europol Regulation are subject to the overall requirements of Article 88(3) of the Treaty on the Functioning of the European Union (TFEU), following which any operational action by Europol must be carried out in liaison and in agreement with the authorities of the Member State concerned, with the application of coercive measures being the exclusive responsibility of the competent*** national authorities.

Or. en

Amendment 1237
Dominik Tarczyński, Beata Kempa, Elżbieta Kruk
on behalf of the ECR Group

Motion for a resolution
Paragraph 176

Motion for a resolution	*Amendment*
176. Europol does not have any autonomous operational powers, and it cannot act without the consent and cooperation of the Member State(s) concerned. ***That presents a problem when there is clear evidence of criminal acts - such as cybercrime, corruption and extortion - but national authorities fail to investigate. This problem is made worse when the Member State authorities are themselves complicit in the crimes.***	176. Europol does not have any autonomous operational powers, and it cannot act without the consent and cooperation of the Member State(s) concerned.

Or. en

Amendment 1238
Gilles Lebreton, Christine Anderson, Mathilde Androuët

Motion for a resolution
Paragraph 176

Motion for a resolution	*Amendment*
176. Europol does not have any autonomous operational powers, and it cannot act without the consent and cooperation of the Member State(s) concerned. ***That presents a problem when there is clear evidence of criminal acts - such as cybercrime, corruption and extortion - but national authorities fail to investigate. This problem is made worse when the Member State authorities are themselves complicit in the crimes***.	176. Europol does not have any autonomous operational powers, and it cannot act without the consent and cooperation of the Member State(s) concerned. ***However, Europol has recently obtained new powers allowing it to pro-actively propose an investigation, even when it concerns a crime committed only in one Member State***.

Or. fr

Amendment 1239
Gilles Lebreton, Christine Anderson, Mathilde Androuët

Motion for a resolution
Paragraph 177

Motion for a resolution	*Amendment*
177. However, Europol has recently obtained new powers allowing it to pro-actively propose an investigation, even when it concerns a crime committed only in one Member State[334], but so far it has been reluctant to make use of those powers. Europol wants to cherish the good relations with the governments, as it fears such an initiative would lead to a breakdown of cooperation in other areas.	***deleted***

[334] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation

(EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation.

Or. fr

Amendment 1240
Sophia in 't Veld

Motion for a resolution
Paragraph 177

Motion for a resolution	*Amendment*
177. However, Europol has recently obtained new powers allowing it to pro-actively propose an investigation, even when it concerns a crime committed only in one Member State[334] ***, but*** so far ***it has been reluctant*** to make use of those powers. Europol wants to cherish the good relations with the governments, as it fears such an initiative would lead to a breakdown of cooperation in other areas.	177. However, Europol has recently obtained new powers allowing it to pro-actively propose an investigation, even when it concerns a crime committed only in one Member State[334]***.There is ample reason for Europol to propose an investigation into the use of, and trade in spyware, with a significant number of Member States involved.Even though a Member State can still refuse a proposal for an investigation by Europol, the onus will be on the Member State to refuse.*** So far ***Europol has refused*** to make use of those powers***. Instead of proposing investigations, in its response to Parliament Europol essentially claims that its new powers may not be in line with the Treaties***. Europol wants to cherish the good relations with the governments, as it fears such an initiative would lead to a breakdown of cooperation in other areas. ***Europol's refusal to act amounts to dereliction of duty.***
[334] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of	[334] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of

criminal investigations, and Europol's role in research and innovation.	criminal investigations, and Europol's role in research and innovation.

Or. en

Amendment 1241
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Lucia Vuolo, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 177

Motion for a resolution	*Amendment*
177. ***However,*** Europol has recently obtained ***new*** powers allowing ***it to pro-actively*** propose ***an*** investigation, even when it concerns a crime committed only in one Member State[334] ***, but so far it has been reluctant to make use of those powers***. Europol ***wants to cherish the good relations with the governments, as it fears such an initiative would lead to a breakdown of cooperation in other areas***.	177. Europol has recently obtained powers allowing ***the Agency to*** propose ***to initiate, conduct or coordinate a criminal*** investigation ***to the competent authorities in the Member States***, even when it concerns a crime committed only in one Member State ***and at the same time affecting a common interest covered by a Union policy***. ***However,*** Europol ***cannot interfere or challenge the decision-making at national level and must act within the scope of Article 88(3) of the TFEU and Article 3 of TEU fulfilling its supportive role***.

[334] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation.

Or. en

Amendment 1242
Dominik Tarczyński, Beata Kempa, Elżbieta Kruk
on behalf of the ECR Group

Motion for a resolution

Paragraph 177

Motion for a resolution	*Amendment*
177. However, Europol has recently obtained new powers allowing it to pro-actively propose an investigation, even when it concerns a crime committed only in one Member State[334] ***, but so far it has been reluctant to make use of those powers.*** Europol ***wants to cherish the good relations with the governments, as it fears such an initiative would lead to a breakdown of cooperation in other areas***.	177. However, Europol has recently obtained new powers allowing it to pro-actively propose an investigation, even when it concerns a crime committed only in one Member State[334]***. However, according to its mandate,*** Europol ***cannot act against the will of the authorities of a Member State***.
[334] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation.	[334] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation.

Or. en

Amendment 1243
Cornelia Ernst, Stelios Kouloglou, Giorgos Georgiou, Anne-Sophie Pelletier

Motion for a resolution
Paragraph 177

Motion for a resolution	*Amendment*
177. ***However,*** Europol has recently obtained new powers allowing it to pro-actively propose an investigation, even when it concerns a crime committed only in one Member State[334] , but so far it has been reluctant to make use of those powers. Europol wants to cherish the good relations with the governments, as it fears such an initiative would lead to a breakdown of cooperation in other areas.	177. Europol has recently obtained new powers allowing it to pro-actively propose an investigation, even when it concerns a crime committed only in one Member State[334] , but so far it has been reluctant to make use of those powers. Europol wants to cherish the good relations with the governments, as it fears such an initiative would lead to a breakdown of cooperation in other areas.
[334] Regulation (EU) 2022/991 of the	[334] Regulation (EU) 2022/991 of the

European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation.	European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation.

Or. en

Amendment 1244
Dominik Tarczyński, Beata Kempa, Elżbieta Kruk
on behalf of the ECR Group

Motion for a resolution
Paragraph 178

Motion for a resolution	*Amendment*
178. On 28 September 2022, PEGA wrote a letter to Europol[335] , urging it to make use of its new powers under Article 6 of the Europol Regulation[336] . In a letter of reply dated 13 October 2022[337] , Europol stated that it has 'contacted five Member States to ascertain whether there is relevant information available at the national level for Europol and whether there is an ongoing or envisaged criminal investigation (or, instead, another inquiry under the applicable provisions of national law). One of the five Member States has meanwhile confirmed to Europol the initiation of criminal investigations under the oversight of the competent judicial authorities, and this has also been verified by Eurojust'. It is not known which countries the letter refers to, nor whether the aforementioned criminal inquiry by one Member State concerns the abuse of spyware by EU Member State governments or by third countries.	***deleted***

335

https://twitter.com/EP_PegaInquiry/status/1576855144574377984

*[336] **"where the Executive Director considers that a criminal investigation should be initiated into a specific crime which concerns only one Member State but affects a common interest covered by a Union policy, he or she may propose to the competent authorities of the Member State concerned, via its national unit, to initiate, conduct or coordinate such a criminal investigation."***

*[337] **File no 1260379.***

Or. en

Amendment 1245
Sophia in 't Veld

Motion for a resolution
Paragraph 178

Motion for a resolution	*Amendment*
178. On 28 September 2022, PEGA wrote a letter to Europol[335] , urging it to make use of its new powers under Article 6 of the Europol Regulation[336] . In a letter of reply dated 13 October 2022[337] , Europol stated that it has 'contacted five Member States to ascertain whether there is relevant information available at the national level for Europol and whether there is an ongoing or envisaged criminal investigation (or, instead, another inquiry under the applicable provisions of national law). One of the five Member States ***has meanwhile*** confirmed to Europol the initiation of criminal investigations under the oversight of the competent judicial authorities, and this has also been verified by Eurojust'. It is not known which countries the letter refers to, nor whether the aforementioned criminal ***inquiry*** by one Member State ***concerns*** the abuse of spyware by EU Member State governments or by third countries.	178. On 28 September 2022, PEGA wrote a letter to Europol[335] , urging it to make use of its new powers under Article 6 of the Europol Regulation[336] . In a letter of reply dated 13 October 2022[337] , Europol stated that it has 'contacted five Member States to ascertain whether there is relevant information available at the national level for Europol and whether there is an ongoing or envisaged criminal investigation (or, instead, another inquiry under the applicable provisions of national law). ***Four of the five Member States have responded to Europol's letter, none of which would have 'relevant information that is available for Europol'. By October 2022,*** one of the five Member States ***had*** confirmed to Europol ***'***the initiation of criminal investigations under the oversight of the competent judicial authorities, and this has also been verified by Eurojust'. ***By December 2022, a second Member State informed Europol 'that one criminal procedure was initiated in connection with the suspected unlawful use of***

Pegasus software which meanwhile was closed by the responsible judicial authorities in that country.' A third Member State notified Europol that 'pre-trial proceedings have been opened in one instance at the regional level', and inquired 'whether Europol holds information on the use of Pegasus software in the respective country, of relevance to the pre-trial proceedings.' A fourth Member State informed Europol 'that there is no criminal investigation ongoing or envisaged', but that 'judicial investigations had been initiatied'.

It is not known which countries the letter refers to, nor whether the aforementioned criminal ***procedures by two Member State, pre-trial proceedings*** by one Member State***, and judicial investigations by another Member State concern*** the abuse of spyware by EU Member State governments or by third countries.

---

335 https://twitter.com/EP_PegaInquiry/status/1576855144574377984

336 "where the Executive Director considers that a criminal investigation should be initiated into a specific crime which concerns only one Member State but affects a common interest covered by a Union policy, he or she may propose to the competent authorities of the Member State concerned, via its national unit, to initiate, conduct or coordinate such a criminal investigation."

337 File no 1260379.

---

335 https://twitter.com/EP_PegaInquiry/status/1576855144574377984

336 "where the Executive Director considers that a criminal investigation should be initiated into a specific crime which concerns only one Member State but affects a common interest covered by a Union policy, he or she may propose to the competent authorities of the Member State concerned, via its national unit, to initiate, conduct or coordinate such a criminal investigation."

337 File no 1260379.

Or. en

Amendment 1246
Carles Puigdemont i Casamajó

Motion for a resolution
Paragraph 178

Motion for a resolution	*Amendment*
178. On 28 September 2022, PEGA wrote a letter to Europol[335] , urging it to make use of its new powers under Article 6 of the Europol Regulation[336] . In a letter of reply dated 13 October 2022[337] , Europol stated that it has 'contacted five Member States to ascertain whether there is relevant information available at the national level for Europol and whether there is an ongoing or envisaged criminal investigation (or, instead, another inquiry under the applicable provisions of national law). One of the five Member States has meanwhile confirmed to Europol the initiation of criminal investigations under the oversight of the competent judicial authorities, and this has also been verified by Eurojust'. It is not known which countries the letter refers to, nor whether the aforementioned criminal inquiry by one Member State concerns the abuse of spyware by EU Member State governments or by third countries.	178. On 28 September 2022, PEGA wrote a letter to Europol[335] , urging it to make use of its new powers under Article 6 of the Europol Regulation[336] . In a letter of reply dated 13 October 2022[337] , Europol stated that it has 'contacted five Member States to ascertain whether there is relevant information available at the national level for Europol and whether there is an ongoing or envisaged criminal investigation (or, instead, another inquiry under the applicable provisions of national law). One of the five Member States has meanwhile confirmed to Europol the initiation of criminal investigations under the oversight of the competent judicial authorities, and this has also been verified by Eurojust'. It is not known which countries the letter refers to, nor whether the aforementioned criminal inquiry by one Member State concerns the abuse of spyware by EU Member State governments or by third countries. ***Moreover, Eurojust should clarify if it was informed of the spying on citizens in third countries inside the European Union.***
335 https://twitter.com/EP_PegaInquiry/status/1576855144574377984	335 https://twitter.com/EP_PegaInquiry/status/1576855144574377984
336 "where the Executive Director considers that a criminal investigation should be initiated into a specific crime which concerns only one Member State but affects a common interest covered by a Union policy, he or she may propose to the competent authorities of the Member State concerned, via its national unit, to initiate, conduct or coordinate such a criminal investigation."	336 "where the Executive Director considers that a criminal investigation should be initiated into a specific crime which concerns only one Member State but affects a common interest covered by a Union policy, he or she may propose to the competent authorities of the Member State concerned, via its national unit, to initiate, conduct or coordinate such a criminal investigation."
337 File no 1260379.	337 File no 1260379.
	Or. en

Amendment 1247
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Lucia Vuolo, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 178

Motion for a resolution	*Amendment*
178. On 28 September 2022, PEGA wrote a letter to Europol[335] , urging it to make use of its new powers under Article 6 of the Europol Regulation[336] . In a letter of reply dated 13 October 2022[337] , Europol stated that it has 'contacted five Member States to ascertain whether there is relevant information available at the national level for Europol and whether there is an ongoing or envisaged criminal investigation (or, instead, another inquiry under the applicable provisions of national law). One of the five Member States has meanwhile confirmed to Europol the initiation of criminal investigations under the oversight of the competent judicial authorities, and this has also been verified by Eurojust'. It is not known which countries the letter refers to, nor whether the aforementioned criminal inquiry by one Member State concerns the abuse of spyware by EU Member State governments or by third countries.	178. On 28 September 2022, PEGA wrote a letter to Europol[335] , urging it to make use of its new powers under Article 6 of the Europol Regulation[336] . In a letter of reply dated 13 October 2022[337] , Europol stated that it has 'contacted five Member States to ascertain whether there is relevant information available at the national level for Europol and whether there is an ongoing or envisaged criminal investigation (or, instead, another inquiry under the applicable provisions of national law). One of the five Member States has meanwhile confirmed to Europol the initiation of criminal investigations under the oversight of the competent judicial authorities, and this has also been verified by Eurojust'. It is not known which countries the letter refers to ***as Europol cannot unilaterally disclose this information***, nor whether the aforementioned criminal inquiry by one Member State concerns the abuse of spyware by EU Member State governments or by third countries.
335 https://twitter.com/EP_PegaInquiry/status/1576855144574377984	335 https://twitter.com/EP_PegaInquiry/status/1576855144574377984
336 "where the Executive Director considers that a criminal investigation should be initiated into a specific crime which concerns only one Member State but affects a common interest covered by a Union policy, he or she may propose to the competent authorities of the Member State concerned, via its national unit, to initiate, conduct or coordinate such a criminal investigation."	336 "where the Executive Director considers that a criminal investigation should be initiated into a specific crime which concerns only one Member State but affects a common interest covered by a Union policy, he or she may propose to the competent authorities of the Member State concerned, via its national unit, to initiate, conduct or coordinate such a criminal investigation."

[337] File no 1260379.

[337] File no 1260379.

Or. en

Amendment 1248
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 179

Motion for a resolution	*Amendment*
179. The EU turns out to be quite powerless against potential criminal activity by national authorities, even if it affects the EU.	***deleted***

Or. en

Amendment 1249
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Lucia Vuolo, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 180

Motion for a resolution	*Amendment*
180. Paradoxically, contrary to Europol, the US is actively investigating the use of spyware in the EU. On 5 November 2022, it was reported that the FBI visited Athens to investigate 'how far the illegal surveillance has spread and who trafficked it.'[338] .	***deleted***

[338] https://insidestory.gr/article/ti-ekane-i-epitropi-pega-gia-tis-ypoklopes-stin-athina?token=4U1KNVW1DQ

Or. en

Amendment 1250
Dominik Tarczyński, Beata Kempa, Elżbieta Kruk
on behalf of the ECR Group

Motion for a resolution
Paragraph 180

Motion for a resolution	*Amendment*
180. Paradoxically, contrary to Europol, the US is actively investigating the use of spyware in the EU. On 5 November 2022, it was reported that the FBI visited Athens to investigate 'how far the illegal surveillance has spread and who trafficked it.'[338] .	***deleted***

[338] https://insidestory.gr/article/ti-ekane-i-epitropi-pega-gia-tis-ypoklopes-stin-athina?token=4U1KNVW1DQ

Or. en

Amendment 1251
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 180 a (new)

Motion for a resolution	*Amendment*
	180 a. EU funding in third countries

Or. en

Amendment 1252
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 180 b (new)

Motion for a resolution	*Amendment*
	180 b. On 28 November 2022, the EU Ombudsman concluded that the European Commission failed to sufficiently assess the human rights risks before providing support to African countries to develop surveillance capabilities, notably in the context of the EU Emergency Trust Fund for Africa (EUTFA). The conclusions followed from a complaint by several civil society organisations. In Niger, the Fund allocated €11.5 million for supply with surveillance equipment, including surveillance software, a wiretapping centre, and an international mobile subscriber identity (IMSI) catcher[338a], despite repression against activists in the country. To address the identified shortcomings she identified, the Ombudsman recommended made a suggestion for improvement to ensure that for future EU Trust Fund projects, there is a prior human rights impact assessment to take place[338b].
	[338a] https://ec.europa.eu/trustfundforafrica/sites/default/files/final_t05-eutf-sah-ne-05_eci_avenant_1.pdf
	[338b] European Ombudsman, How the European Commission assessed human rights impacts before providing support to African countries to develop surveillance capabilities. https://www.ombudsman.europa.eu/en/case/en/60368
	Or. en

Amendment 1253
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 180 c (new)

Motion for a resolution	*Amendment*
	180 c. The claim has been made that countries heavily dependent on foreign aid for their national budgets are high consumers of spyware technology, notably Rwanda.[338c] The question is what fundamental rights and rule of law guarantees exist in Union development policies and to what extent development aid can be given if it is used for or enables acquisition of spyware by the receiving country.
	338c
	https://www.theguardian.com/commentisfree/2021/jul/23/rwanda-pegasus-surveillance

Or. en

Amendment 1254
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 180 d (new)

Motion for a resolution	*Amendment*
	180 d. The main legislative instrument within the development policies is Regulation (EU) 2021/947 - the 'Global Europe Regulation'. According to Article 3(1)(a) one of the general objectives is to 'uphold and promote the Union's values, principles and fundamental interests worldwide'.

Or. en

Amendment 1255
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 180 e (new)

Motion for a resolution	*Amendment*
	180 e. According to Article 8(1) in the Global Europe Regulation, the 'Union shall seek to promote, develop and consolidate the principles of democracy, good governance, the rule of law, respect for human rights'. Article 8(2) further states that the Regulation shall be applied with 'a rights-based approach encompassing all human rights, whether civil and political or economic, social and cultural in order to integrate human rights principles, to support the right holders in claiming their rights'.

Or. en

Amendment 1256
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Marcel Kolaja, Jordi Solé
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 180 f (new)

Motion for a resolution	*Amendment*
	180 f. Union funding may be provided through the types of financing envisaged by the Financial Regulation. As the respect for democracy, human rights and the rule of law is essential for sound financial management and effective Union funding as referred to in the Financial Regulation, assistance could be suspended in the event of degradation in democracy, human rights or the rule of law in third countries (Recital 40).

Or. en

Amendment 1257
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 180 g (new)

Motion for a resolution	*Amendment*
	180 g. Persons and entities implementing financial instruments and budgetary guarantees shall comply with applicable Union law and principles and agreed international and Union standards as laid down in Article 155(2) and (3) of the Financial Regulation. The Commission shall assess whether the systems, rules and procedures of those persons and entities ensure protection of the financial interests of the Union equivalent to that provided for where the Commission implements the Union budget, with due regard to the principle of proportionality, taking into account the nature of the action and the conditions under which this action is implemented. Moreover, the Global Europe Regulation foresees, in Article 20, an incentive-based approach, stating that the progress of the partner countries shall be regularly assessed, in particular by means of progress reports, which include trends as compared to previous years.

Or. en

Amendment 1258
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 180 h (new)

Motion for a resolution	*Amendment*
	180 h. It appears that more stringent control mechanisms should be implemented to ensure that financing from the Union development aid should not serve to fund or to facilitate the purchase of tools that could impinge on the principles of democracy, good governance, the rule of law and respect for human rights. Therefore, assessments of the compliance with the Financial Regulation made by the Commission should contain specific control criteria to avoid such abuses.

Or. en

Amendment 1259
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 180 i (new)

Motion for a resolution	*Amendment*
	180 i. The possible consequences resulting from a lack of oversight and assessment in funding could not only result in human rights violations in third countries but also impact the EU's own cybersecurity capacities. Therefore, any funding of surveillance technology, including research funding via Horizon 2020 with third countries (ie. Israel), need to be accompanied with appropriate safeguards in their funding programs.

Or. en

Amendment 1260
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja

on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 180 j (new)

Motion for a resolution	*Amendment*
	180 j. Regulation (EU) 2021/695 establishes Horizon Europe. According to Article 19 "Actions carried out under the Programme shall comply with ethical principles and relevant Union, national and international law, including the Charter and the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Supplementary Protocols." Furthermore, the Annotated Model Grant Agreement describes the main ethical principles that should be respected. In relation to surveillance and spyware, the main ethical principles are: Respecting human dignity and integrity; Ensuring privacy and confidentiality; Promoting justice and inclusiveness.

Or. en

Amendment 1261
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Marcel Kolaja, Jordi Solé
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 180 k (new)

Motion for a resolution	*Amendment*
	180 k. The European Commission published a guidance note on potential misuse of research on 7 January 2020. In this regards, it considers that the research most vulnerable to misuse is, among others, research that involves developing surveillance technologies that could curtail human rights and civil liberties. It provides measures to take to address potential misuse of projects when

planning research applications.

Or. en

Amendment 1262
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 180 l (new)

Motion for a resolution	*Amendment*
	180 l. The claim has been made that Horizon 2020 and Horizon Europe funds have gone to technologies used in spyware. It is clear that funds have been made available to military and security companies, including Israeli defence companies Elbit and Israel Aerospace Industries[338d].
	338d ***https://www.euractiv.com/section/innovation-industry/news/meps-denounce-eu-funding-of-israeli-defence-firms/ and https://euobserver.com/opinion/154902***

Or. en

Amendment 1263
Hannah Neumann, Saskia Bricmont, Gwendoline Delbos-Corfield, Diana Riba i Giner, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 180 m (new)

Motion for a resolution	*Amendment*
	180 m. The European Commission has stated that it has not found any evidence that would confirm the allegation that Horizon 2020 funds had been used to

finance technologies developed by NSO Group[338e].

338e

https://www.europarl.europa.eu/doceo/document/E-8-2018-006103-ASW_EN.html

Or. en

Amendment 1264
Dominik Tarczyński, Beata Kempa, Elżbieta Kruk
on behalf of the ECR Group

Motion for a resolution
Paragraph 181

Motion for a resolution	*Amendment*
181. The Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) ***play an important role in defending democracy, the rule of law and fundamental rights. However, they*** can only act upon a complaint or pre-judicial question. Proceedings are very lengthy and offer little concrete remedy in individual cases. Over the years, the courts have created a vast body of relevant case law, for example establishing standards for surveillance. ***However, these courts have no means to ensure that their ruling are enforced.*** So far, one complaint about the illegitimate use of spyware has been submitted to the ECtHR[339] . ***However, the road to the Strasbourg or Luxembourg courts is often long, costly, and cumbersome, as all options for national judicial proceedings must first be exhausted. This is especially the case if national prosecutors or judges fail or refuse to take a case, the bar for passing the admissibility test is high.***	181. The Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) can only act upon a complaint or pre-judicial question. Proceedings are very lengthy and offer little concrete remedy in individual cases. Over the years, the courts have created a vast body of relevant case law, for example establishing standards for surveillance. So far, one complaint about the illegitimate use of spyware has been submitted to the ECtHR[339] .
[339] Appeal by Koukakis to the European Court of Human Rights, 27 July 2022.	[339] Appeal by Koukakis to the European Court of Human Rights, 27 July 2022.

Or. en

Amendment 1265
Sophia in 't Veld

Motion for a resolution
Subheading 129 a (new)

Motion for a resolution	*Amendment*
	Ombudsman

Or. en

Amendment 1266
Sophia in 't Veld

Motion for a resolution
Paragraph 181 a (new)

Motion for a resolution	*Amendment*
	181 a. On 28 November 2022, the Ombudsman concluded that the Commission failed to protect human rights in its development funding for surveillance measures in third countries.[1a] Although not directly related to spyware, it indicates that the Commission turns a blind eye to the importance of human rights protection in the area of surveillance.
	[1a] https://www.ombudsman.europa.eu/en/decision/en/163491

Or. en

Amendment 1267
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Andrzej Halicki, Bartosz Arłukowicz, Radosław Sikorski, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Subheading 130 a (new)

Motion for a resolution	*Amendment*
	Redress on the EU level

Or. en

Amendment 1268
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Henna Virkkunen, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution
Paragraph 182

Motion for a resolution	*Amendment*
182. The European Data Protection Board, the European Data Protection Supervisor, the EU Ombudsman, the European Court of Auditors and Eurojust have few competences to scrutinise or intervene in case of illegitimate use of, or trade in spyware by Member State governments. ***Some of their members may indeed be involved in the scandals in their Member State of origin, and in covering them up. Additionally, this may have an impact on the functioning and the integrity of these EU bodies.*** The European Public Prosecutor's Office could potentially intervene when EU money is involved in any way.	182. The European Data Protection Board, the European Data Protection Supervisor, the EU Ombudsman, the European Court of Auditors and Eurojust have few competences to scrutinise or intervene in case of illegitimate use of, or trade in spyware by Member State governments. The European Public Prosecutor's Office could potentially intervene when EU money is involved in any way.

Or. en

Amendment 1269
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 182 a (new)

Motion for a resolution	*Amendment*
	182 a. As reported by Ilia Siatitsa, Programme Director and Senior Legal Officer, Privacy International, during the PEGA Committee Hearing on "Spyware used in third countries and implications for EU foreign relations", held last 15th ***December 2022, a 2020 Privacy International investigation[339a] revealed hundreds of documents detailing surveillance techniques used in trainings organised by the European Union Agency for Law Enforcement Training in order to train authorities in the Balkans, Middle East, and Northern Africa in controversial phone and internet surveillance techniques. Such documents disclosed a training session provided by Policia Nacional, the national police force of Spain, to police, security, and intelligence authorities in Bosnia and Herzegovina (federal as well as those based in Republika Srpska) on financial investigations similarly outlined potential avenues for tracking IP addresses, emails, and conducting wiretapping. The training documents provided by Policia Nacional were promoting the use of malware or computer trojans into devices to extract data and take control of functions such as the camera and microphone, and sold on the open market by companies such as NSO Group.***
	[339a] https://privacyinternational.org/long-read/4289/revealed-eu-training-regime-teaching-neighbours-how-spy
	Or. en

Amendment 1270
Vladimír Bilčík, Juan Ignacio Zoido Álvarez, Andrzej Halicki, Bartosz Arłukowicz, Radosław Sikorski, Elissavet Vozemberg-Vrionidi, Gabriel Mato, Karolin Braunsberger-Reinhold

Motion for a resolution

Paragraph 182 a (new)

Motion for a resolution	*Amendment*
	182 a. Citizens of all Member States are also European citizens and therefore the EU should ensure that their rights, as enshrined in the EU Charter of Fundamental Rights, are protected. Given that in some Member States victims of illegal surveillance have no access to an effective redress, the EU should be committed to setting up an independent body that would help victims, or those who suspect that they might have been victims, to find out if their devices have been hacked. Such body should provide technical and IT support as well as legal advice to victims; furthermore, it should serve as a European think tank and should assist the EU institutions in developing common EU standards for the use of operational tools in full respect of EU laws and values.

Or. en

Amendment 1271
Radosław Sikorski, Bartosz Arłukowicz, Andrzej Halicki

Motion for a resolution
Paragraph 182 a (new)

Motion for a resolution	*Amendment*
	182a. Victims of Pegasus and equivalent surveillance spyware should have the right to know what happened to the data illegally taken from their devices, whether it is stored, disseminated, prepared or used in any way. The individuals concerned should have control over this data.

Or. pl

Amendment 1272
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 182 b (new)

Motion for a resolution	*Amendment*
	182 b. Legal aspects of the use of spyware

Or. en

Amendment 1273
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 182 c (new)

Motion for a resolution	*Amendment*
	182 c. Several fundamental rights enshrined in the Charter may be affected by the use of spyware. First of all, such use may interfere with the right to privacy, family life and confidentiality of communications (Article 7). It may also interfere with the right to data protection (Article 8)[339b] and the right to freedom of expression guaranteed in Article 11, which constitutes one of the essential foundations of a pluralist, democratic society. The right to property (Article 17) could be affected by the placing of spyware on a targets phone. Furthermore, equality before the law (Article 20) and non-discrimination (Article 21) could be affected, and, the right to a fair trial (Article 47) may also be compromised. Spyware can also have chilling effects on other human rights and fundamental freedoms, including the right to dignity (Article 1), freedom of assembly (Article 12), freedom of religion (Article 11), and even the physical and psychological

integrity of an individual (Article 3).

[339b] ***The right to data protection is also laid down in Article 16 of the Treaty on the Functioning of the European Union (TFEU), and in Article 39 of the Treaty on the European Union (TEU) and in secondary legislation.***

Or. en

Amendment 1274
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Jordi Solé, Gwendoline Delbos-Corfield, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 182 d (new)

Motion for a resolution	*Amendment*
	182 d. Article 52(1) of the Charter lays down the conditions for the limitation of the exercise of fundamental rights. A limitation must be provided for by law[339c], respect the essence of the rights and freedoms concerned, be subject to the principle of proportionality[339d], and only be imposed if it is necessary (strict necessity[339e]) and genuinely meets objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others[339f].

[339c] ***Judgment of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, para 175***

[339d] ***Judgment of 8 April 2014, Digital Rights Ireland and Others, C-293/12 and C-594/12, EU:C:2014:238***

[339e] ***idem***

[339f] ***Judgment of 15 February 2016, N., C601/15 PPU, EU:C:2016:84, para 50***

Or. en

Amendment 1275
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 182 e (new)

Motion for a resolution	*Amendment*
	182 e. The CJEU acknowledges that a serious threat to national security that is genuine, present or foreseeable could justify very serious interferences with fundamental rights, subject to strict conditions and safeguards. Similarly, the prevention of serious crimes, could justify such interference[339g] . It should be noted that where a suspicion of such a treat is clearly defined in time, such as with rest of terrorist attacks, it is known when a suspect has been radicalised, the interference cannot encompass data from before the radicalisation.
	[339g] Judgment of 6 October 2020, La Quadrature du Net and Others, C-511/18, C-512/18 and C-520/18, EU:C:2020:791, para 156

Or. en

Amendment 1276
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 182 f (new)

Motion for a resolution	*Amendment*
	182 f. However, the interference must be proportionate given the seriousness of the interference and the importance of the

public interest objective pursued[339h]. Given the level of interference with the right to privacy, it is highly questionable if spyware such as Pegasus could meet the requirements of proportionality, irrespective of whether the measure can be deemed necessary to achieve the legitimate objectives of a democratic state[339i] . This is especially true taking into account that such spyware is not limited to classical wiretapping, as the control over the mobile system allows access not only to incoming/outgoing conversations, but also to all messages, log calls, images and documents on a phone, allowing to build a full profile of a victim through his/her past communications and interactions. Moreover, not only direct victims have their rights affected, but also potentially all their contacts. Therefore, the interference to the right to privacy can be considered even more serious.

[339h] idem, para 131

[339i] EDPS Preliminary remarks on Modern Spyware, edps.europa.eu, page 8.

Or. en

Amendment 1277
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 182 g (new)

Motion for a resolution	*Amendment*
	182 g. Article 4 (2) TEU provides that "national security remains the sole responsibility of each EU Member State". That responsibility of Member States corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses "the prevention

and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities".

Or. en

Amendment 1278
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 182 h (new)

Motion for a resolution	*Amendment*
	182 h. Secondary law, such as GDPR and the e-Privacy Directive (ePD), goes further as they set out an exclusion for national security. The Law Enforcement Directive (LED) does not apply to activities that falls outside the scope of Union law, but as Article 4(2) TEU is not an exclusion, Union law still applies. In the EU legal order, while national security remains the sole responsibility of the Member States, Union law still applies, as confirmed recently by the CJEU[339j]. More specifically, a specific rule on national security is applicable only in practices that are purely governmental, without the involvement of any private actor[339k]. For clarity, it should be noted that the use of spyware for crime prevention is covered by the e-Privacy Directive and LED.

[339j] Privacy International, para 44 and La Quadrature du Net and Others, para 99.

[339k] Privacy International, para 35 and La Quadrature du Net and Others, para 92.

Or. en

Amendment 1279
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 182 i (new)

Motion for a resolution	*Amendment*
	182 i. The ECtHR has repeatedly addressed the use of targeted communication surveillance and indiscriminate/bulk interception of communication data surveillance in law enforcement activities. In this respect, it has developed its own standard for assessing national legislation, which also includes a list of legal safeguards that should be applied to reduce the risk of abuse of power[339l]. Any interference to these rights is only permitted if it is prescribed by law, pursues one of the legitimate aims set out in the Convention, is necessary in a democratic society and is proportionate to the legitimate aims pursued.
	[339l] See cases: Big Brother Watch and Others v. the United Kingdom [GC], no. 58170/13, 25 May 2021; Centrum för rättvisa v. Sweden, [GC], no. 35252/08, 25 May 2021

Or. en

Amendment 1280
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 182 j (new)

Motion for a resolution	*Amendment*
	182 j. It also considers that the notion of national security should be clearly interpreted by domestic law and provide the scope of offences/crimes threatening the national security as well as other severe or exceptionally severe crimes allowing authorities to use secret surveillance measures to effectively prevent those crimes

Or. en

Amendment 1281
Hannah Neumann, Saskia Bricmont, Diana Riba i Giner, Gwendoline Delbos-Corfield, Jordi Solé, Marcel Kolaja
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 182 k (new)

Motion for a resolution	*Amendment*
	182 k. State authorities are under an obligation to ensure effective mechanisms (including national courts, supervisory/monitoring mechanisms, public scrutiny) for avoiding arbitrariness and securing a fair balance between the right to privacy and the legitimate aim pursued by the interference. In order to assess the necessity and reasonableness of any intrusion in the private life or communication, any communication tapping or secret surveillance should be authorised by an independent and impartial domestic authority being vested with the relevant mandate and independent oversight should be ensured.

Or. en