2023-01-12 // drs. Lucas van der Hoeven (www.cbsm.nl // lucas.van.der.hoeven @cbsm.nl)

PEGASUS, PREDATOR en ANDERE BEDREIGINGEN VOOR DE RECHTSSTAAT

De speciale VN-rapporteur over vrijheid van meningsuiting acht het gebruik van spyware door regeringen gevaarlijk vanwege de kans op buitengerechtelijke, standrechtelijke of willekeurige executies, moorden of verdwijningen van personen.

"Het Griekse afluisterschandaal kan wel eens groter zijn dan destijds het Amerikaanse Watergate", meent D66-Europarlementariër Sophie in 't Veld. Uit recent 'Pegasus' onderzoek kwam naar voren dat ten minste 14 staatshoofden en 180 journalisten uit 20 landen tussen 2016 en juni 2021 het doelwit waren van het Israëlische software bedrijf NSO, de maker van 'spyware'. Ook Europese overheden bespioneren vrijwel ongemerkt journalisten en politieke mede- en tegenstanders, waaronder journalisten van Al Jazeera, CNN, de Financial Times, de Associated Press, The New York Times, The Wall Street Journal, Bloomberg News en Le Monde.

In Polen en Hongarije, zei In 't Veld, is spyware een "integraal element" van een methodisch systeem "ontworpen om burgers te controleren en zelfs te onderdrukken"

Vooral in Spanje en Griekenland zijn deze afluisterpraktijken in de openbaarheid gekomen. Het Europese Parlement vroeg Sophie in 't Veld (D66) een verkennend onderzoek te doen naar de achtergronden van deze spionage-schandalen. Zij schreef met haar collega's Jeroen Lenaers (CDA) en Thijs Reuten (PvdA) een onthutsende rapportage. Kennisname van de illegale afluisterpraktijken in Spanje en Griekenland zijn ook voor Nederland van belang, maar ook de gevolgen van de mogelijke uitbreiding van het takenpakket van Interpol. Maar nog meer vanwege de lopende herziening van de Wet op de Inlichtingen- en Veiligheidsdiensten (de WIV). Door het steeds verder aanscherpen van de bevoegdheden tot het afluisteren, dreigen de vrijheden van burgers steeds meer te worden ingeperkt. De mogelijke negatieve gevolgen voor de eigen privacy in ruimste zin zijn groot. Overigens maakte Nederland al gebruik van Pegasus en wel bij de opsporing en arrestatie van de crimineel Riduan Taghi in Dubai in 2019.

Pegasus en Predator

Het Israëlische cyberwapenbedrijf NSO Group ontwikkelde Pegasus spyware. Deze kan heimelijk worden geïnstalleerd op de meeste mobiele telefoons en andere apparaten. Pegasus kan iOS-versies tot 14.7 exploiteren (???) via een 'zero-click-exploit'; dus het apparaat kan ongemerkt voor de gebruiker worden geactiveerd. Vanaf 2022 is deze module zelfs in staat om sms-berichten te lezen, oproepen te volgen, wachtwoorden te verzamelen, locaties te bepalen, toegang te krijgen tot de microfoon en camera van het doelapparaat en informatie uit de geïnstalleerde apps te verzamelen. Deze software is niet detecteerbaar. Slechts het Canadese Citizen-Lab in Toronto is in staat om deze ínfectie' aan toonbaar te maken. Uit hun analyses komt naar voren dat wereldwijd – van Thailand tot Mexico - onwelgevallige antiregime-activisten, journalisten en politieke leiders uit de hele wereld.

Sophie in 't Veld: "We moeten erkennen dat alle lidstaten over spyware beschikken, ook al geven ze dat niet toe".

In juli 2021 meldde het Pegasus Project, een internationaal onderzoeksinitiatief van meer dan 80 journalisten in samenwerking met Amnesty International, dat Pegasus nog steeds op grote schaal werd gebruikt. Hun rapport 'Forensic Methodology Report: How to catch NSO Group's Pegasus' vermeldt dat tussen 2014 en juli 2021 allerlei aanvallen plaatsvonden. In juli 2021 publiceerden zij een 'Pegasus'-software lijst met meer dan 50.000 telefoonnummers

uit 50 landen. Deze nummers waren van politici, mensenrechtenactivisten, journalisten, advocaten en politieke dissidenten, waaronder de in 2017 vermoorde Mexicaanse journalist Cecilio Pineda en naasten van de vermoorde journalist Jamal Khashoggi uit Saoedi-Arabië.

Sophie in 't Veld: "Met spionagesoftware zoals Pegasus kunnen mobiele telefoons op afstand worden overgenomen. Camera en microfoon kunnen worden aangezet en alle berichten, foto's en contacten ingezien. Echt problematisch is dat deze spyware niet alleen gebruikt wordt voor het opsporen van criminelen en terroristen maar ook voor overheidsoptreden tegen gewone burgers, journalisten, politieke tegenstanders, rechters en activisten".

In 2020 stapte Pegasus over op 'zero-click exploits' en 'netwerk-gebaseerde' aanvallen. Via deze methoden kunnen klanten inbreken in doeltelefoons zonder gebruikersinteractie of detecteerbare sporen achter te laten. In december 2020 bleek dat 36 telefoons van medewerkers van Al Jazeera en van een Londense journalist van Al Araby TV gehackt. Alle telefoons werden gevolgd vanuit 4 afzonderlijke clusters van servers van NSO Group, die waarschijnlijk met Saoedi-Arabië en de Verenigde Arabische Emiraten zijn verbonden.

Spanje's 'Catalangate'

Volgens The Guardian en El País maakte de Spaanse regering gebruik van Pegasus om de telefoons van 63 Catalaanse en Baskische politici en journalisten af te luisteren. Op 5 mei 2022 gaf de Spaanse minister van Defensie Margarita Robles toe dat zij 20 mensen in de gaten had gehouden die betrokken waren bij de Catalaanse onafhankelijkheidsbeweging. Maar ook de smartphones van premier Pedro Sánchez en de minister van Defensie zelf werden afgetapt. De spionage wordt toegeschreven aan Marokkaanse opdrachtgevers, vanwege de diplomatieke spanningen tussen beide landen. Deze onthullingen veroorzaakten een crisis in het Spaanse parlement. De partij van Pedro Sánchez sprak zijn veto uit tegen een parlementair onderzoek naar het Pegasus-schandaal. Daarop dreigde de Catalaanse Onafhankelijkheids Partij zijn parlementaire steun aan de minderheidsregering van Sánchez in te trekken. Het hoofd van de Spaanse geheime dienst (CNI), Paz Esteban, gaf toe dat haar bureau 18 Catalaanse onafhankelijkheidsleiders had bespioneerd. (Zo bevonden zich onder de 63 bespioneerden, de voorzitter van het parlement van Catalonië Roger Torrent; voormalig parlementsleden van Catalonië en Baskenland. Na haar bekentenis werd het hoofd van de geheime dienst afgezet. Op 29 november vond een hoorzitting in het Europees Parlement plaats, waarbij de nieuwe chef van de inlichtingendienst, Esperanza Casteleiro werd ondervraagd. Zij beperkte zich tot het uitleggen van het wettelijke kader waaronder de Spaanse geheime diensten opereren. Op de 28 vragen van Eu-parlementsleden gaf ze geen enkel antwoord: alles is naar haar zeggen in wezen geheim.

Griekse 'Watergate'

Op het gebied van mediavrijheid stond Griekenland in 2021 op de 108ste plaats in de ranglijst van "Reporters Without Borders". Een daling van 38 plaatsen in een jaar, waarmee Griekenland binnen de EU de slechtste prestatie ooit heeft geleverd. Griekenland gaat niet alleen gebukt onder economische tegenspoed, maar ook onder een groot afluisterschandaal. Hierbij zijn premier Mitzotakis, ministers, veiligheidsdiensten en parlementariërs betrokken. Inmiddels denkt 64% van de Grieken dat hun premier is betrokken in het 'Griekse Watergate'. Mitzotakis zelf beweert van niets te weten. Dat is onwaarschijnlijk, aangezien hij bij zijn aantreden in 2019 een wet liet aannemen waarbij hij de geheime diensten onder zijn persoonlijke bevoegdheid plaatste. De affaire explodeerde in juli 2022 toen Nikos Androulakis – prominent lid van het Europees Parlement en leider van de Griekse Socialistische Partij – een klacht indiende vanwege pogingen om zijn mobiele telefoon en die van twee journalisten af te tappen met behulp van Predator-spyware. De beruchte Israëlische spyware werd gebruikt door de staatsinlichtingendienst EYP.

Androulakis zegt: "het Europees Verdrag voor de Rechten van de Mens zijn geschonden en start dus een procedure bij het EU-Hof" .

Invloedrijke leden van de conservatieve Nieuwe Democratie-partij en potentiële rivalen voor een toekomstig leiderschapsverkiezing behoorden tot de doelwitten. Zelfs de voormalige conservatieve premier Samaras, de huidige minister van buitenlandse zaken Dendias en Griekse generale staf werden bespioneerd. Vervolgens namen de secretaris van premier Mitsotakis en Grigoris Dimitriadis, neef van de premier én hoofd van de geheime dienst, ontslag. Intussen gelastte het Griekse Hooggerechtshof een afluisteronderzoek, waarbij onder meer de voormalige premier Antonis Samaras, huidige leden van het kabinet en scheepsmagnaat Vangelis Marinakis, eigenaar van de voetbalclubs Olympiakos en Nottingham Forest het doelwit waren. Intussen heeft het Griekse Hooggerechtshof een onderzoek gelast naar deze spionage- affaire, waarbij meer dan 30 Griekse politici, journalisten en zakenlieden werden afgeluisterd. Op 28 november hield de onderzoekscommissie van het Griekse parlement een cruciale vergadering. Deze commissie beslist of Grigoris Dimitriadis, de voormalige stafchef en neef van de Griekse premier, zal moeten getuigen. Als blijkt dat hij op de hoogte was van deze gang van zaken, zal de regering waarschijnlijk moeten aftreden.

Italian Justice Minister Carlo Nordio: "The Italian government is looking to reform the use of wiretapping as the practice costs millions and is often used as a means to pressure political opponents, including via the press".

Op 4 november 2022 bezocht de 'afluister'-commissie van het Europees Parlement Griekenland. EP-lid Sophie in 't Veld concludeerde: "Ik zie geen krachtige zoektocht naar daders. Deze zaak moet dringend en volledig opgehelderd zijn vóór de (Griekse) verkiezingen van volgend jaar". Commissievoorzitter Jeroen Lenaers voegde toe: "Veel van onze vragen moeten nog worden beantwoord". Wel benadrukte hij dat er in ieder geval drie beleidsmaatregelen moeten worden getroffen, zoals een Europese regulering van deze sector, Europese import- en exportregels voor aankoop van zulke technologieën en Europese transparantieregels en minimumnormen voor aankoop en gebruik van spyware door overheden. In 't Veld pleit voor Europese handhaving, wet- en regelgeving voor legitiem gebruik van spionagesoftware, maar tevens het aan banden leggen van illegaal gebruik. Geen van beiden pleiten zij voor een spyware-vrije Unie. Wel bepleiten zij strenger toezicht op de verschillende producenten, zoals de Israëlische leveranciers NSO en Candiru, het Cypriotische Intellexa Alliance, het Italiaanse Tyke- en RCSlab, het Oostenrijkse DSIRF en het Duitse FinFisher.

Interpol

De bevoegdheden van Interpol werden eerder dit jaar uitgebreid. De opgerekte bevoegdheden bestaan uit de verwerking en analyse van gegevens van burgers die geen enkel misdrijf begingen. "Vroeger was dat niet mogelijk, nu is het toegestaan", zegt Chloe Barthélemy, senior beleidsadviseur bij de in Brussel gevestigde European Digital Rights. Interpol is verwikkeld in allerlei schandalen, zoals het delen met de Duitse politie van de privé-gegevens van de Nederlandse vredesactivist Frank van der Linde. Deze laatste vroeg om een kopie, waarop Interpol zijn gegevens wiste, wat in strijd is met de EU-regels voor gegevensbescherming. Europol is ook betrokken bij een ander dataschandaal waarbij grenswachten van Frontex de databank van Europol met details over ongewenste migranten vulden. Frontex negeerde waarschuwingen van hun eigen functionaris voor gegevensbescherming over 'functie-misbruik'. "Wij zien een groot risico voor de rechtsstaat", aldus Barthélemy. Zij wijst daarbij op een algemene trend waarbij voorspellend politiewerk grotendeels berust op uitgebreide gegevensverzameling. Met behulp van algoritmes kunnen deze bulkgegevens worden geanalyseerd. Dit leidt tot massa surveillance op basis van

criteria zoals bijvoorbeeld land van herkomst, migratiestatus, geslacht of welk ander willekeurig gekozen kenmerk. Hierdoor worden burgerrechten ingeperkt, waarbij dient te worden uit gegaan van onschuldigheid, het recht op privacy en het discriminatieverbod. "Wij zien deze uitbreiding van het EU-politiewerk als een echte bedreiging voor de rechtsstaat", meent Laure Baudrihaye-Gerard, juridisch directeur van de NGO 'Fair Trials'. Instanties voor wetshandhaving dienen geen 'blanco cheque' te krijgen. "Deze instellingen moeten ter verantwoording kunnen worden geroepen". Ook Saskia Bricmont van de Europese Groene partij vindt dat er zorgwekkende hiaten zijn in het toezicht op Europol en Frontex. Beiden werken immers op het gebied van wetshandhaving én migratie. Dit kan problemen opleveren: zo zou een illegale migrant die aangifte doet bij de politie in België of Nederland, ongevraagd zijn persoonsgegevens kenbaar maken aan de immigratieautoriteiten. Ook de beperking van het delen van biometrische gegevens met Turkije en Egypte werd eerder dit jaar verder afgezwakt door de medewetgevers. In een rapport van Statewatch, een burgerrechtenorganisatie, staat dat Europol mogelijk zal worden misbruikt "als een kanaal om politieke tegenstanders en dissidenten lastig te vallen". Zowel Turkije als Egypte kennen een lange geschiedenis van het uitvaardigen van arrestatiebevelen tegen tegenstanders en critici van hun regeringen.

Herziening Nederlandse afluisterwet

De overheid wil de Wet op de Inlichtingen- en Veiligheidsdiensten (de WIV) uit 2018 opnieuw aanpassen. Deze 'sleepwet' stuitte destijds op veel tegenstand. In het daarna gehouden raadgevend referendum stemde de meerderheid van de burgers tegen het wetsvoorstel. De overheid breidde de WIV daarna met enige artikelen uit, zodat de burgerrechten beter worden beschermd. In maart 2021 besloot de regering deze wet echter opnieuw aan te willen passen. Daardoor zal de bindende TIB-toets (Toetsingscommissie Inzet Bevoegdheden) ***vooraf*** worden veranderd in een bindend CTIVD (Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten) toezicht ***tijdens*** de uitoefening van bevoegdheden. Dit vereist een andere, veel intensievere samenwerking en informatie-uitwisseling tussen TIB en CTIVD. Het wetsvoorstel is onvoldoende helder met betrekking tot het vermelden van technische risico's in verzoeken. Gedurende de voorgestelde toestemmingsperiode kan de bevoegdheid zonder voorafgaande toets worden uitgebreid door zogenaamd "bijschrijven". De kabelbevoegdheid wordt uitgebreid met het interveniëren van internetverkeer van streamingsdiensten en binnenlands internetverkeer. Tegen de voorgestelde herziening maken vooral de toezichthouder bezwaar. Mr. Moussault, TIB voorzitter, verwerpt het voorstel omdat de huidige vooraf te geven toestemming tot afluisteren dan zal worden omgezet in een toetsing achteraf. Toch lijkt een definitief wetsvoorstel dichtbij.

Conclusie:

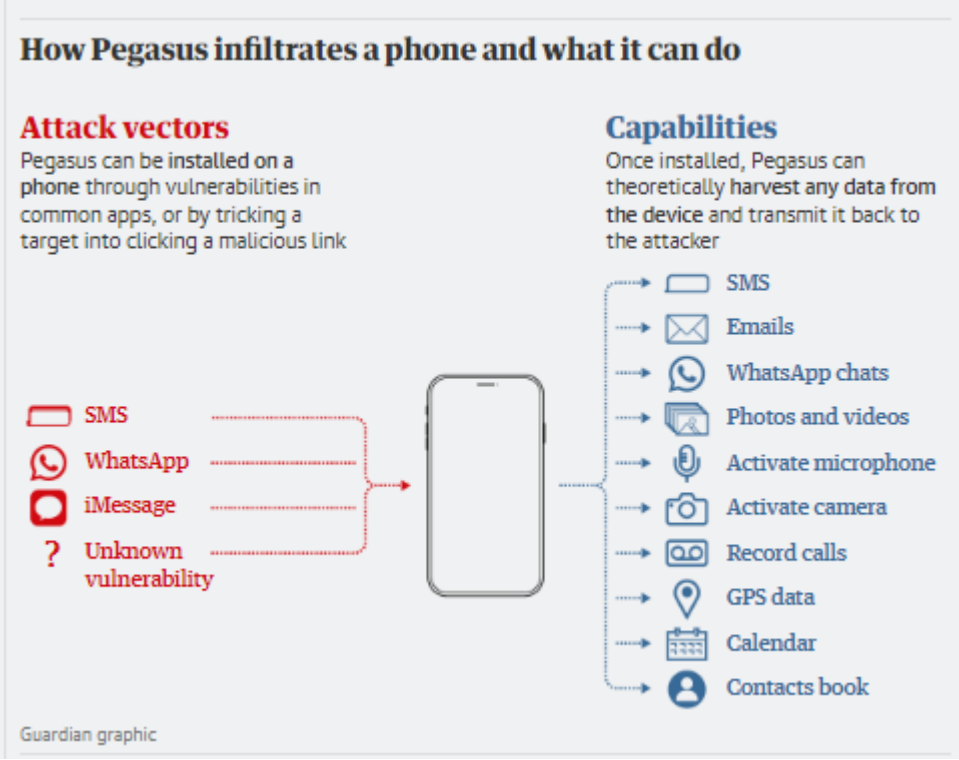
Door het gebruik van allerlei spionage software, uitbreiding van bevoegdheden van Interpol en de Wet op de Inlichtingen- en Veiligheidsdiensten, dreigen de vrijheden van burgers steeds te worden ingeperkt. De mogelijke gevolgen zijn onder meer inbreuken op privacy, gezinsleven, communicatie en data-bescherming. Ook het recht op vrije meningsuiting en democratische waarden komen er door onder druk te staan; evenals het recht op niet-discriminatie, bijeenkomen en eerlijke rechtspleging. Maar vooral ook het recht van individuele burgers op religieuze, fysieke en psychologische integriteit. Alleen door het stellen van wettelijke grenzen en strikt toezicht kunnen die uitholling van vrijheden worden beperkt. Het EU-rapport van D66-Europarlementariër Sophie in 't Veld spoort politici aan tot het aanscherpen van anti-spionage wetgeving en strikter toezicht op ongebreidelde data gebruik door opsporingsdiensten, waardoor burgerlijke vrijheden verder worden beknot.

==========

newsroom@freedomvoicesnetwork.org

Bronnen:

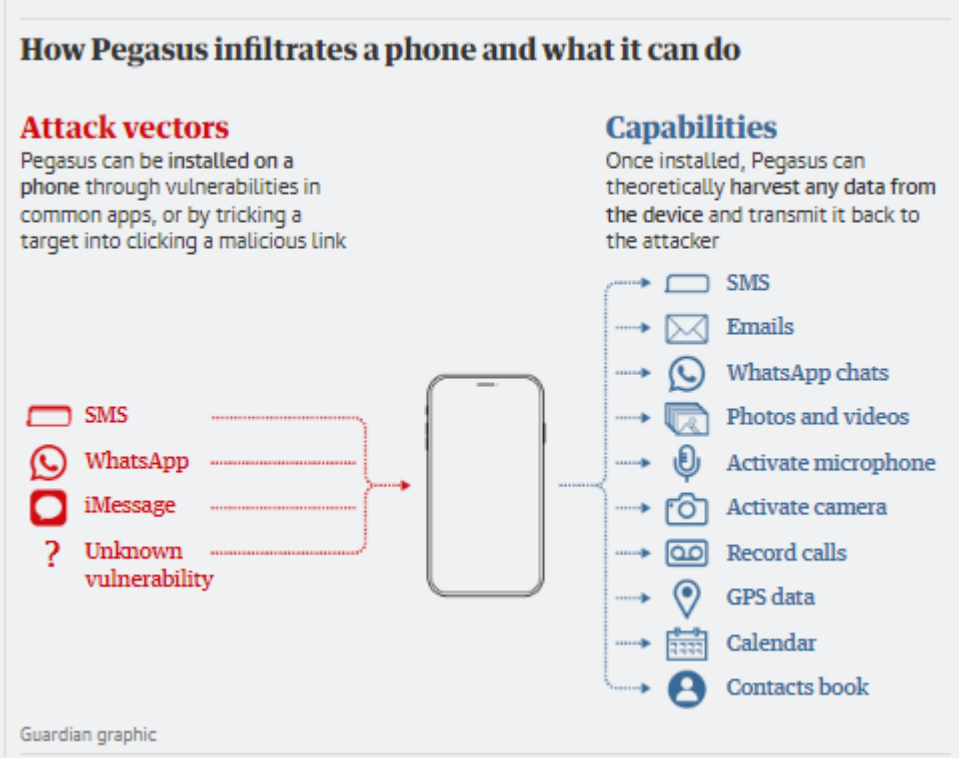
- *2022-11-29 In 't Veld - PEGA-draft-report-final-8-11-2.pdf*
- *Sophie in 't Veld (sophieintveld.eu)*
- *10-11-2022: Europol given 'blank cheque' to do what it wants, say critics (euobserver.com)*
- *https://en.wikipedia.org/wiki/Ridouan_Taghi*
- *Greeks unconvinced PM was not aware of illegal spyware surveillance – EURACTIV.com*
- *https://nl.wikipedia.org/wiki/Pegasus_Project*
- *Pegasus (spyware) - Wikipedia*
- *https://www.amnesty.org/en/latest/news/2022/04/spain-pegasus-spyware-catalans-targeted/*
- *https://www.amnesty.org/en/latest/news/2022/07/the-pegasus-project-one-year-on-spyware-crisis-continues-after-failure-to-clamp-down-on-surveillance-industry*
- *https://forbiddenstories.org/pegasus-project-impacts-map*
- *https://forbiddenstories.org/pegasus-project-articles*
- *Pegasus: EU in need to step up as a citizens' rights guarantor – EURACTIV.com*
- *https://nl.wikipedia.org/wiki/Wet_op_de_inlichtingen-_en_veiligheidsdiensten_2017*
- *file:///C:/Users/lucas/Downloads/Brief+aan+BZK+en+DEF+mbt+Reactie+op+het+concept+wetsvoorstel+Tijdelijke+wet+onderzoek+AIVD+en+MIVD+naar+landen+met+een+offensief+cyberprogramma.pdf*
- *https://www.tib-ivd.nl/documenten/brieven/2022/04/14/reactie-tib-concept-wetsvoorstel-tijdelijke-wet*
- *All questions and no answers, as Spanish spy chief stays mute on Pegasus hacking scandal | Euronews*
- *https://en.wikipedia.org/wiki/CatalanGate*
- *Revealed: leak uncovers global abuse of cyber-surveillance weapon | Surveillance | The Guardian*
- *file:///C:/Users/lucas/Downloads/Brief+aan+BZK+en+DEF+mbt+Reactie+op+het+concept+wetsvoorstel+Tijdelijke+wet+onderzoek+AIVD+en+MIVD+naar+landen+met+een+offensief+cyberprogramma.pdf*
- *https://www.ctivd.nl*
- Italy to reform wiretapping practices amid safety concerns – EURACTIV.com



==========

Individuals in Spain whose phones were infected or targeted with Pegasus

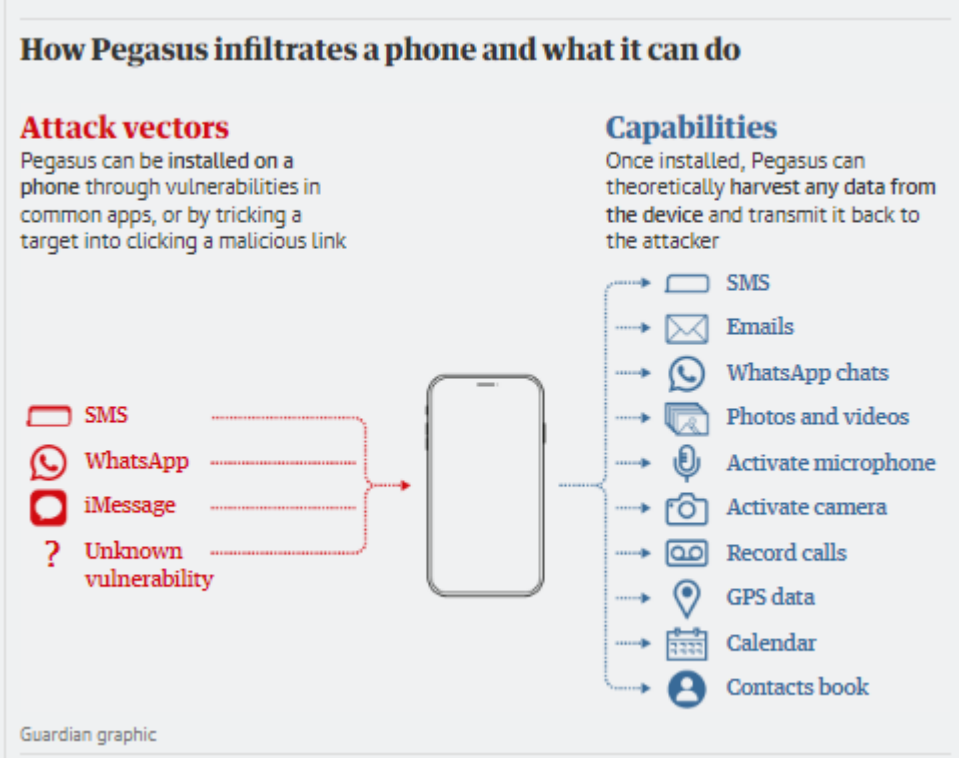
Type	Names



==========

Individuals in Spain whose phones were infected or targeted with Pegasus

Type	Names
Politicians	Pere Aragonès, Elsa Artadi, Albert Batet, Ferran Bel, David Bonvehi, Laura Borràs, Albert Botran, Meritxell Budo, Joan Ramon Casals, Antoni Comín, Josep Costa, David Fernández, Anna Gabriel, Jon Iñarritu, Josep Maria Jové, Joaquim Jubert, Ernest Maragall, Artur Mas, Miriam Nogueras, Arnaldo Otegi, Marta Pascal, Diana Riba, Josep Rius, Carles Riera, Marta Rovira, Sergi Sabrià, Oriol Sagrera, Meritxell Serret, Jordi Solé, Marc Solsona, Joaquim Torra, Roger Torrent, Xavier Vendrell
Political activists and lawyers	Arià Bayé, Alba Bosch, Jordi Bosch, Gonzalo Boye, Jaume Alonso Cuevillas, Jordi Domingo, Elena Jimenez, Marcel Mauri, Sergi Miquel, Elisenda Paluzie, Olivier Peter, Jordi Sanchez, Sònia Urpí, Andreu Van den Eynde, 4 anonymous activists/lawyers
Government officials	Pol Cruz, Fernando Grande-Marlaska (reported by El Confidencial), Luis Planas (reported by El Confidencial), Margarita Robles (reported by The Guardian)
Academics	Josep Lluís Alay, Fernando Grande-Marlaska, Maria Cinta Cid, Josep Ma



==========

Individuals in Spain whose phones were infected or targeted with Pegasus

Type	**Names**
	Ganyet
Journalists	Meritxell Bonet, Albano Dante Fachin, Marcela Topor
Businesspeople	David Madi, Dolors Mas, Joan Matamala
Head of state	Pedro Sánchez (reported by, - among others, The Guardian)
Others	Jordi Baylina, Pau Escrich

==========

- file:///C:/Users/lucas/Downloads/Brief+aan+BZK+en+DEF+mbt+Reactie+op+het+concept+wetsvoorstel+Tijdelijke+wet+onderzoek+AIVD+en+MIVD+naar+landen+met+een+offensief+cyberprogramma.pdf
  p. 6

2.6. Overzicht

De belangrijkste wijzigingen in het wetsvoorstel die een verruiming van bevoegdheden van de diensten tot gevolg hebben staan hieronder uitgewerkt in een tabel.

Wiv 2017	**Tijdelijke wet**
Bijschrijfmogelijkheid alleen voor exclusief in gebruik zijnde infrastructuur	Bijschrijfmogelijkheid ook voor gehackte servers, thuisrouters en andere apparaten
Maximale termijn beoordeling relevantiebepaling 1,5 jaar, zo spoedig mogelijk uitvoeren, niet bindend toezicht CTIVD	Beoordeling op relevantie niet langer zo snel mogelijk, geen maximale termijn, bindend toezicht CTIVD
Verkennen gegevensstromen kabelinterceptie gericht en ter verificatie	Verkennen gegevensstromen kabelinterceptie ongericht en ten behoeve van verkenning
Kabelinterceptie voor inlichtingenwerk alleen onderzoeksopdrachtgericht	Ongerichte kabelinterceptie voor inlichtingenwerk
Kabelinterceptie van verkeer streamingsdiensten en Nederland-Nederlandverkeer (buiten cyber defence onderzoek) direct vernietigd	Kabelinterceptie van verkeer streamingsdiensten en Nederland-Nederlandverkeer