THE PREDATOR FILES: CAUGHT IN THE NET

THE GLOBAL THREAT FROM "EU REGULATED" SPYWARE

AMNESTY INTERNATIONAL

Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

First published in 2023
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Index: ACT 10/7245/2023
Original language: English

amnesty.org

Cover image: © Colin Foo

AMNESTY INTERNATIONAL

CONTENTS

GLOSSARY

TERM	DEFINITION
SPYWARE	*Spyware* is software which enables an operator to gain covert access to information from a target computer system or device.
COMMERCIAL SPYWARE	*Commercial or mercenary spyware* are surveillance products developed and sold by corporate actors to governments to conduct surveillance operations. So called "end-to-end" commercial spyware systems provide a full system for device infection and data collection. Components of these systems include the exploits used to install the spyware, a spyware agent which runs on the target device after infection and backend systems to gather and analyse the collected surveillance data.
SPYWARE AGENT	A *spyware agent* (or implant) is the final software code installed on a computer or phone after it has been successfully infected. The agent is responsible for collecting data from the device, activating sensors such as microphones and cameras, and uploading this data to the spyware operator.
SOFTWARE VULNERABILITY	A *software vulnerability* is a technical flaw or weakness in a software component or piece of code which can be exploited by an attacker to bypass security defences.
EXPLOIT	An *exploit* is a piece of software or code which takes advantage of (or exploits) one or more software vulnerabilities to gain access to a device. On modern mobile devices exploits must bypass numerous layered security defences and can be highly complex. A full exploit chain targeting latest device versions can sell for millions of euros.
BASEBAND	A mobile *baseband* is the hardware and software components in a mobile phone which are responsible for communicating over a radio interface with a mobile phone cell tower or base station.
ZERO-DAY	A *zero-day vulnerability* is a software flaw which is not known to the original software developer and for which a software fix is not available. A zero-day exploit taking advantage of this flaw can successfully target even fully patched and updated devices.
VECTOR	*Vector* is a surveillance industry term for the different pathways or techniques which can be used to deliver an exploit to a target device. These include so called *1-click* and *zero-click* vectors.
1-CLICK	A *1-click* attack requires action from the target to enable the infection of their device, typically by opening a malicious link. Various social engineering techniques are used to trick the target into opening the link, including spoofing legitimate websites or news articles. If clicked on, the attack link loads an exploit chain to first compromise the web browser and ultimately install the spyware agent on the target device.

TERM	DEFINITION
ZERO-CLICK	A *zero-click* attack is a surveillance industry marketing term for any vector which can infect a device without requiring a user action, such as clicking on a link. *Fully remote* zero-click attacks allow infection over the internet, often by exploiting flaws in popular messaging apps such as iMessage or WhatsApp. Non-remote or *tactical* zero-click attacks can silently infect devices where the attacker has privileged network access or is in physical proximity to the target.
NETWORK INJECTION	*Network injection* is a technique where internet data packets are injected in the internet traffic of a target to block, intercept or manipulate their traffic.
MAN-IN-THE-MIDDLE (MITM)	A *man-in-the-middle* is an attacker who can read, modify, and block the network traffic from a target. A MiTM capability can be used to censor the target or perform network injection attacks.
MAN-ON-THE-SIDE (MOTS)	A *man-on-the-side* is an attacker who can read and monitor network traffic but is not able to directly block or modify the traffic. This situation is common when an attacker has access to a copy or mirror of traffic sent over a fibre optic link. Network injection attacks can also be performed from this network position.
TACTICAL INFECTION	A *tactical infection vector* allows an attacker to attack devices in close physical proximity. Malicious Wi-Fi networks and mobile base stations can be used to silently redirect a nearby target to an exploit link. Attackers can also exploit vulnerabilities in cellular baseband software and Wi-Fi interfaces to infect nearby devices using radio packets sent over the air.
STRATEGIC INFECTION	*Strategic infection* is a marketing term referring to network injection systems deployed at an ISP (internet service provider) or national internet gateway which can be used to deliver spyware. These systems can intercept unencrypted requests sent by a target and silently redirect their device to an exploit link.
SS7	*Signaling System Number 7* is a set of signalling protocols and standards used in telephone networks to perform actions such as call-establishment, routing, and roaming between national and international mobile phone providers. The protocol was designed without modern security defences and has been exploited by commercial surveillance vendors to enable various attacks including location tracking and communications interception.
DISTRIBUTED DENIAL OF SERVICE (DDOS)	A *Distributed Denial* of Service is an attack aimed at disrupting a website or network by overloading the system with too much traffic or too many requests. This attack can result in a website being unavailable to legitimate visitors.
AVATAR	An *Avatar* is a fake identity or online account which is used to gather information from online platforms or to interact with a targeted user. These seemingly real profiles can be used to send targeted attack links or to spread information online through social media or messaging services.

TABLE 1: SUMMARY OF COMPANIES

The Intellexa alliance, its subsidiaries and partnerships have evolved over time since its inception into a complex worldwide company structure. For readability purposes, both EIC and Amnesty International use the following breakdown:

Nexa group – Nexa Technologies (France),[1] Nexa Technologies CZ s.r.o (Czech Republic), Advanced Middle East Systems (United Arab Emirates), Trovicor fz (United Arab Emirates).[2]

Intellexa group – Wispear/Passitora (Cyprus),[3] Cytrox (North Macedonia),[4] Cytrox Holdings Zrt (Hungary), Intellexa S.A(Greece),[5], Intellexa ltd(Ireland),[6] Thalestris ltd(Ireland).[7]

Intellexa alliance[8] – is a technological and commercial alliance concluded in 2019 between the Intellexa group and the Nexa group. The two groups of companies maintained a separate shareholding. In the press release announcing the birth of the alliance, the member companies were Nexa Technologies, Advanced Middle East Systems, Cytrox, WiSpear and Senpai Technologies.[9] It is unclear whether the alliance between the Nexa group and the Intellexa group is still active today.

The Intellexa group of companies was founded in 2018 by the former Israeli army officer Tal Dilian and several of his associates, which sells the Predator spyware. Since 2020, it has been controlled by the holding company Thalestris, which is based in Ireland. The Intellexa group's main companies are Cytrox (North Macedonia), which develops the Predator spyware system, WiSpear (Cyprus), specialist in Wi-Fi interception, and Senpai Technologies (Israel), a specialist in open-source intelligence and the creation of virtual avatars.

The Nexa group of companies, which mainly operated from France, specialized in traffic interception and mass surveillance systems (IP, voice, satellite, IMSI catchers, big data analysis). The group was created in 2012 to take over the surveillance business of the French company Amesys. It included from the start, Nexa Technologies (France) and Advanced Middle East Systems (Dubai), a sister company used by Nexa as a sales office. Between 2019 and 2022, the companies of the Nexa group were controlled by the holding company Boss Industries (France).[10] In 2019, Boss Industries purchased the company Trovicor (Dubai),[11] which specializes in "lawful interception" (telephone monitoring systems). In 2020, the Nexa group decided to abandon Nexa Technologies as a brand and began to operate under the commercial name Trovicor Intelligence.[12]

---

[1] Data INPI, Presentation of the company RB 42, 26 September 2023, https://data.inpi.fr/entreprises/751230681?q=751230681#751230681

[2] Trovicor Intelligence, Legal Disclosure, https://trovicor.com/legal-disclosure/ (accessed on 26 September 2023).

[3] Department of the Registrar of Companies and Intellectual Property, 26 September 2023, https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=%25&number=318328&searchtype=optStartMatch&index=1&lang=EN&tname=%25&sc=1

[4] Central Securities Depository, Известувања за корпоративни настани, https://www.cdhv.mk/известувања_за_корпоративни_настани.aspx (accessed on 26 September 2023).

[5] Athens Chamber of Commerce and Industry, Intellexa ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ, 26 September 2023, https://directory.acci.gr/companies/details/140944573

[6] Companies Registration Office, Intellexa Limited, https://core.cro.ie/e-commerce/company/697890 (accessed on 26 September 2023).

[7] Companies Registration Office, Thalestris Limited, https://core.cro.ie/e-commerce/company/693992 (accessed on 26 September 2023).

[8] Release Wire, "The Intellexa Intelligence Alliance Expands with the Addition of New Members and the Enhancement of Its End-to-End Offering", 20 June 2019, http://www.releasewire.com/press-releases/the-intellexa-intelligence-alliance-expands-with-the-addition-of-new-members-and-the-enhancement-of-its-end-to-end-offering-1234811.htm

[9] Release Wire, "The Intellexa Intelligence Alliance Expands with the Addition of New Members and the Enhancement of Its End-to-End Offering" (previously cited), http://www.releasewire.com/press-releases/the-intellexa-intelligence-alliance-expands-with-the-addition-of-new-members-and-the-enhancement-of-its-end-to-end-offering-1234811.htm

[10] Data INPI, Présentation de l'entreprise BOSS INDUSTRIES, 26 September 2023, https://data.inpi.fr/entreprises/853120541?q=Boss%20Industries%20#853120541

[11] Clairfield, "Clairfield advises Boss Industries on the acquisition of Dubai-based company Trovicor", 17 December 2019, https://www.clairfield.com/clairfield-advises-boss-industries-on-the-acquisition-of-dubai-based-company-trovicor/

[12] Intelligence Online, "France: Nexa renamed RB 42 with new cybersecurity focus", 3 April 2023, https://www.intelligenceonline.com/surveillance--interception/2023/04/03/nexa-renamed-rb-42-with-new-cybersecurity-focus,109930650-art

In 2022 Nexa Technologies sold its assets to the French company ChapsVision,[13] and in 2023 changed its name to RB 42 and announced that it had ceased its activities in the surveillance business.[14] Boss Industries is still the owner of Trovicor, according to public documents.[15]

Cytrox, is a North Macedonian company established in 2017[16] which was the original creator of the Predator spyware and was acquired by WiSpear in 2018.[17]

Amesys, based in France, was a telecom and defence company, which created a mass-monitoring system called Eagle, capable of performing mass surveillance of internet (IP) traffic at the scale of a whole country.[18] Amesys ceased its activities in the cybersurveillance business in 2012, after the transfer of its assets to Nexa Technologies, which renamed Eagle as Cerebro.

[13] Intelligence Online, "France: ChapsVision takes up strong position in interceptions thanks to Elektron takeover", 24 January 2022, https://www.intelligenceonline.com/surveillance--interception/2022/01/24/chapsvision-takes-up-strong-position-in-interceptions-thanks-to-elektron-takeover,109718567-art
[14] Nexa Technologies, Nexa Technologies: Une page se tourne, 2023, https://www.nexatech.fr/fr/about
[15] Boss Industries, *Comptes sociaux,* 2021, p18.
[16] Central Securities Depository, Известувања за корпоративни настани, (previously cited), https://www.cdhv.mk/известувања_за_корпоративни_настани.aspx
[17] Atooro, 25 May 2020, http://web.archive.org/web/20200525234222/http://www.atooro.com/
[18] Privacy International, "Amesys Brochure Eagle", February 2009, https://www.documentcloud.org/documents/409206-95-amesys-critical-system-architect.html

1. EXECUTIVE SUMMARY

Over the past decade, civil society organizations, researchers, and journalists have exposed how governments around the world have been unlawfully targeting activists, journalists, and politicians using tools developed by private cyber-surveillance companies. Amnesty International and numerous civil society organizations have repeatedly warned that states' opaque trade and deployment of privately manufactured surveillance technologies, particularly spyware, have wrought a digital surveillance crisis, which has severely and detrimentally impacted human rights, media freedoms, and social movements across the world. The 2021 Pegasus Project disclosures – which exposed the global scale and breadth of unlawful surveillance facilitated by NSO Group's Pegasus spyware – and subsequent civil society research have forced governments around the world to take note of the massive scale and breadth of spyware abuse, spurring the beginnings of action to rein in some of the most notorious spyware vendors. However, fresh disclosures by Amnesty International, and the findings of the new Predator Files investigation coordinated by European Investigative Collaborations (EIC) media network, have laid bare how government action has been inadequate and ineffective in ending spyware abuse. This report details these findings.

First, as part of the Predator Files investigation, Amnesty International's Security Lab collaborated with EIC, a partnership of European media organizations, as a technical partner. Amnesty International analysed documents accessed by EIC to ascertain the technical specifications of a suite of surveillance products developed, operated, and marketed by the Intellexa alliance – which is an alliance of surveillance technology companies – between 2007 and 2022 (see Chapter 4). Amnesty International found that this includes a host of targeted and mass surveillance technologies.

Targeted surveillance technologies include highly invasive mobile spyware like Predator, which can be delivered to devices using either 1-click attacks or 0-click attacks (see Glossary). The Intellexa alliance also offers various techniques to install the spyware through "tactical attacks", which enable the targeting of devices in close physical proximity. In addition, strategic infection methods have also been developed, operated, and marketed by the Intellexa alliance. These methods allow a state actor to deliver silent infection attempts to users of cooperating internet service providers, or across a whole country if the spyware operator has direct access to internet traffic. Strategic infection systems resemble mass surveillance tools as they require access to large-scale internet traffic to target and infect individuals. The mass and "massive" surveillance products offered by the Intellexa alliance suggest an evolution of earlier surveillance technologies from lawful interception systems that allowed traffic monitoring in a targeted, individualised manner – that potentially allowed for more checks and limitations – to more overbroad and indiscriminate methods.

Amnesty International believes that both types of technologies – highly invasive spyware and indiscriminate mass surveillance tools – are fundamentally incompatible with human rights (see Chapter 3). The Predator spyware, and its rebranded variants, are highly invasive spyware that can access unlimited amounts of data on the device and cannot, at present, be independently audited. As such, Amnesty International's assessment is that no deployment of Predator and other such forms of highly invasive spyware can be human rights compliant, and they should be permanently banned (see Chapter 5).

Second, in this report, Amnesty International has revealed a previously undisclosed targeted surveillance operation by a customer of Intellexa's Predator spyware with connections to Viet Nam. The customer appears to be aligned with government interests in Viet Nam, and between February and June 2023, it targeted at least 50 social media accounts belonging to 27 individuals and 23 institutions, using spyware tools developed and sold by the Intellexa alliance. The targeting was done using 1-click attacks sent to the social media accounts of individuals and institutions from an X (formerly known as Twitter) account called

@Joseph_Gordon16. Those targeted as part of this spyware operation include a Berlin-based independent news website, political figures in the European Parliament, the European Commission, academic researchers, and think-tanks. In addition to these, other attempted targets include United Nations officials, the President of Taiwan, United States senators and representatives, and other diplomatic authorities.

Google's Threat Analysis Group confirmed to Amnesty International that Google's own research had identified that the domains and URLs that Amnesty International discovered as part of the spyware operation were linked to the Intellexa alliance's Predator spyware system. Together with evidence from EIC partners, our findings show evidence of sales of Intellexa alliance's surveillance products to the Vietnamese Ministry of Public Security and suggest that agents of the Vietnamese authorities, or persons acting on their behalf, may be behind the spyware campaign. In addition, Google confirmed to EIC partners that they "associate" the Intellexa Predator campaign and indicators described in this report to "a government actor in Vietnam" (see Chapter 4).

These disclosures are based on ongoing technical research by Amnesty International's Security Lab to monitor the development and deployment of surveillance technologies offered by mercenary spyware companies, including those offered by the Intellexa alliance. As part of these efforts, Amnesty International's analysis of recent technical infrastructure linked to the Predator spyware system also indicates likely active customers or targeting of individuals in Sudan, Madagascar, Kazakhstan, Mongolia, Egypt, Indonesia, Viet Nam, and Angola among others (see Chapter 3).

The findings in this report are also based on an interview with a targeted journalist from Viet Nam, shipment records, trade data, and other EIC research and reporting into the Intellexa alliance's sales of surveillance and infection solutions. Amnesty International also reviewed reports, statements, laws, and studies by UN bodies and experts, regional and various national level authorities, investigative and policy reports by civil society organizations, as well as media reports (see Chapter 2).

Third, this report discusses the human rights implications of the Predator Files disclosures, which show how a suite of highly invasive surveillance technologies supplied by the Intellexa alliance is being sold and transferred around the world with impunity. The Intellexa alliance is comprised of various surveillance vendors with a corporate presence in European Union (EU) member states, as well as other countries around the world (see Table 1). The disclosures show the global scale and breadth of sales of surveillance technologies of just one alliance of surveillance vendors, which has been supplying its wares to Egypt, Libya, Madagascar, Saudi Arabia, Viet Nam, and France among many others between 2007 and 2022. These transfers pose a high likelihood of human rights violations due to past instances of unlawful surveillance in these countries and/or an absence of domestic surveillance safeguards that could prevent these technologies from being unlawfully unleashed on civil society, journalists, or opposition politicians (see Chapter 3).

Fourth, this report details a history of human rights abuses that have been linked to the Intellexa alliance in Greece, Libya, and Egypt. Intellexa advertises itself as an "EU based and regulated company". The Intellexa alliance reportedly comprises of Nexa Technologies and Advanced Middle East Systems (comprising the Nexa group), as well as WiSpear, Cytrox and Senpai Technologies (comprising the Intellexa group). The Nexa and Intellexa groups of companies control multiple corporate entities, some of which have been renamed. The entities span various jurisdictions, both within and outside the EU. The exact nature of links between these companies is shrouded in secrecy, as corporate entities and the structures between them are constantly morphing, renaming, rebranding, and evolving. These opaque and complex corporate structures appear to make it easier for companies to evade accountability, transparency, and government regulation, including regional and national export controls and corporate due diligence mechanisms. In the case of the Intellexa alliance, the picture is even more complex, due to corporate structures of not only one primary company, but its allied surveillance product vendors, its parent companies, and their investors. The convoluted nature of this corporate entity could make accountability and transparency for unlawful targeting using tools of this surveillance alliance even harder (see Table 1 and Chapter 4).

As laid out in the UN Guiding Principles on Business and Human Rights (UN Guiding Principles), companies have a responsibility to respect human rights wherever they operate in the world. In order to meet that responsibility, companies must carry out human rights due diligence. The companies in the Intellexa alliance have themselves not proactively disclosed any information about their human rights due diligence practices. Any assessments, if they exist, about the human rights impacts of their surveillance technologies remain shrouded in secrecy. Nation states also have binding obligations under international human rights law to protect human rights from abuse by third parties. This includes the obligation to regulate the conduct of companies who are domiciled in their territory or are under their effective control in order to prevent them from causing or contributing to human rights abuses even if they occur in other countries. The failure of states to put a meaningful check on the Intellexa alliance, – for example, states where the alliance's

corporate entities are based, which includes Greece, Ireland, France, Germany, Czech Republic, Cyprus, Hungary, Switzerland, Israel, North Macedonia, and the UAE – has led to human rights violations (see Chapter 5).Taken together, the above-mentioned findings show that civil society and journalists continue to face the devastating consequences of unlawful and unchecked use of surveillance technologies, which continue to threaten the rights to privacy, freedom of expression, association, and peaceful assembly of those targeted. In addition, as detailed in this report, the targeting of regional, national, and international official authorities, shows once again that commercial spyware has severe implications both for human rights and the security of the digital ecosystem. Unregulated, these surveillance technologies can and have been turned back on third governments and authorities.

These findings are just the tip of the iceberg. As surveillance companies and their state clients continue to hide behind the rhetoric of national security and confidentiality to evade transparency and accountability, the actual scale and breadth of unlawful targeting using tools supplied by the Intellexa alliance is likely to be much higher. Warnings by civil society and lessons from the Pegasus Project mean that for each of the countries where disclosures reveal that the Intellexa alliance has sold its technologies, civil society could be facing wholesale clandestine surveillance. These new disclosures make clear, yet again, that the unchecked sale and transfer of surveillance technologies could continue to facilitate human rights abuse on a massive global scale, as companies are still being allowed to freely sell and transfer their wares in utmost secrecy. Our findings demonstrate once more that any claims by companies that unlawful targeting is anomalous are decidedly false. Human rights abuse is a feature of the industry, not a bug.

In the aftermath of the Pegasus Project disclosures, states have taken some steps in the right direction to regulate the industry and state-use of these technologies. Some are significant and welcome steps in the right direction. However, public declarations, recommendations, and voluntary commitments have not always translated into action, and those unlawfully targeted with spyware around the world have not yet obtained meaningful accountability or remedies. While some states have initiated voluntary efforts, others have stone-walled investigations and failed to provide meaningful transparency. There need to be more concerted efforts by states to put in place binding and enforceable human rights safeguards at a national, regional and international level. In 2019, the former UN Special Rapporteur on Freedom of Opinion and Expression noted “It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists.” Amnesty International believes that despite initial progress, this is still the case (see Chapter 5).

In particular, the latest disclosures paint a dismal picture of failures of the EU and its member states to rein in unaccountable companies and errant member states, which continue to take advantage of the conspicuously large cracks in the regulatory systems at regional and national levels. The brazen surveillance campaign detailed in this report using the Intellexa alliance's tools shows the very direct risks from the uncontrolled proliferation and transfer of cyber-surveillance tools from countries within the EU. Not only do they lead to human rights abuses abroad, but they are also a threat to security and human rights within the EU.

Exports of spyware from the EU are subject to licensing under the Dual-Use Export Regulation, which should, in theory, take account of human rights risks posed by such exports. The “Predator Files” disclosures, however, demonstrate that export licences for surveillance technologies were granted by member states when there was a substantial risk of human rights violations by the end users. Disclosures also show that EU export control regulations were circumvented through opaque corporate structures and entities in third countries. It is clear that the EU Dual-Use Export Regulation has significant shortcomings. Two years after the publication of the Recast Dual Use regulation, it has not been robustly and transparently implemented. The European Parliament’s Pegasus and other Equivalent Spyware Investigation Committee (PEGA Committee) also pointed to the lack of political will of the EU and member states. While ongoing legislative efforts like the Corporate Sustainability Due Diligence Directive (CSDDD) offer a timely opportunity to begin to address the harms of the targeted surveillance sector, the loopholes in the proposals put forward by the EU co-legislators could mean the CSDDD is not properly applied to surveillance technology companies (see Chapter 6).

Key recommendations to States

In light of the ineffectiveness of the current regulation, as well as the intrinsically abusive nature of Predator, all states should:

- (Particularly states that have granted export licences) Immediately revoke all marketing and export licences issued to the Intellexa alliance and conduct an independent, impartial, transparent investigation to determine the extent of unlawful targeting, to culminate in public statement on results of efforts and steps to prevent future harm.

- Enforce a ban on the use of highly invasive spyware. Such spyware cannot, at present, be independently audited or limited in its functionality to only those functions that are necessary and proportionate to a specific use and target.
- Implement a human rights regulatory framework that governs surveillance and that is in line with international human rights standards. Until such a framework is implemented, a moratorium on the purchase, sale, transfer, and use of all spyware should be enforced.
- Implement domestic legislation that imposes safeguards against human rights violations and abuses through digital surveillance and establish accountability mechanisms designed to provide victims of surveillance abuses a pathway to remedy.
- Legally require surveillance companies to conduct human rights due diligence in relation to their global operations, including on the use of their products and services.

Key recommendations to the European Union and its Member States

- EU member states and the European Commission should ensure the robust implementation of the 2021 EU Export Control Rules. This includes taking immediate action towards underscoring the human rights due diligence obligations that follow from the Dual-Use Regulation and creating a transparent market in cybersurveillance technologies that is bound by effective human rights safeguards.
- EU member states must adopt and enforce legislation that requires all corporate actors to respect human rights and implement human rights due diligence measures in line with the UN Guiding Principles. As part of the ongoing deliberations on the Corporate Sustainability Due Diligence Directive (CSDDD), the EU should require companies to conduct human rights due diligence with respect to the full value chain including the purchase, sale, transfer, export and use of products. Companies operating in all sectors should implement the requirements on the CSDDD including those producing spyware, as well as financial institutions.

Key recommendations to the government of Viet Nam

The Government of Viet Nam should conduct an independent, impartial, and transparent investigation into the unlawful targeted surveillance mentioned in this report, including investigating whether there are links between this spyware campaign and any specific government agencies.

Key recommendations to the Intellexa alliance

The Intellexa alliance should cease the production and sale of Predator, or any other similar highly invasive spyware that does not include technical safeguards allowing for its lawful use under a human right respecting regulatory framework. It should also provide adequate compensation or other forms of effective redress to victims of unlawful surveillance.

2. METHODOLOGY

This report builds on ongoing technical research by Amnesty International to monitor the development and deployment of surveillance technologies, including targeted mobile spyware, which pose a threat to human rights defenders and civil society globally.[19] This work includes identifying and tracking the evolution of surveillance products offered by mercenary spyware companies such as NSO Group, the Intellexa alliance, and others.[20] The Security Lab has closely tracked Intellexa's Predator spyware since September 2021, enabling the identification of civil society victims of Predator in multiple countries. This technical research led Amnesty International to the identification of a public X (formerly, Twitter) account sharing Intellexa spyware infection links in April 2023, which is fully documented as a case study in this report.

Amnesty International interviewed a journalist originally from Viet Nam, who is now based in Germany, and whose media platform was targeted as part of this spyware attack campaign in February 2023. Amnesty International also identified shipment records and trade data and reviewed an analysis of other Intellexa alliance corporate records obtained by EIC which document sales of the Intellexa alliance's surveillance and infection solutions. The organisation also reviewed reports, statements, laws, and studies by UN bodies and experts, regional and various national level authorities, investigative and policy reports by civil society organizations, as well as media reports.

In addition, as part of the Predator Files investigation, Amnesty International's Security Lab collaborated as a technical partner with European Investigative Collaborations (EIC), a partnership of European media organizations. This report contains findings from Amnesty International's research analysing the technical specifications of a suite of surveillance products offered by the Intellexa alliance of surveillance companies. To do this, Amnesty International analysed marketing brochures and technical documents accessed by EIC, to ascertain the technical capabilities and analyse the human rights implications of the suite of surveillance products that were developed, operated, and marketed by the Intellexa alliance between 2007 and 2022.

Amnesty International sent a letter requesting response to this report's findings to Viet Nam's Ministry of Public Security on 19 September 2023 but did not receive a response at the time of publication. Amnesty International also sent letters requesting a response to these findings to representatives of the Intellexa group and the Nexa group on 20 September 2023. The changing and often deliberately opaque corporate structures of many of these companies – discussed below – made outreach challenging. Amnesty International reached out to the latest corporate entities for some of these companies based on publicly available information contained in various corporate registries or their websites (see Table 1 for an explanation of the corporate entities). Amnesty International asked the entities for information about their human rights due diligence practices. We also asked the companies about steps they took to provide remedy to those affected by the use of their technologies that have been revealed in previous investigative reports but did not receive a response at the time of publication. On 26 September 2023, Amnesty International also wrote to Delsons Hong Kong Limited about our findings on shipments of surveillance technologies to Viet Nam, outlined in section 4.5 below. We did not receive a response at the time of publication.

---

[19] Amnesty International, "Forensic Methodology Report: How to catch NSO Group's Pegasus", 18 July 2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[20] See for example, Amnesty International, "Amnesty International uncovers new hacking campaign linked to mercenary spyware company", 29 March 2023, https://www.amnesty.org/en/latest/news/2023/03/new-android-hacking-campaign-linked-to-mercenary-spyware-company/

While Amnesty International did not receive a direct reply from the Intellexa or Nexa groups, former Nexa group executives and main shareholders sent a response to EIC partners on behalf of their companies including Nexa Technologies and Advanced Middle East Systems. Part of their response covered their involvement in sales to Viet Nam, and has been incorporated in Section 4.5, below.

Amnesty International extends its deepest gratitude to everyone who participated in this research, in particular our partners in EIC and to Khoa Lê Trung. Amnesty International Security Lab's is also grateful to the Digital Security Lab at Reporters Without Borders for their assistance in collecting forensic information during this investigation. Amnesty International thanks Citizen Lab for their independent verification of our findings connecting identified attack domains to Intellexa's Predator spyware, and the Google Threat Analysis Group[21] for sharing their research into the surveillance infrastructure of the Intellexa alliance.

DIGITAL SECURITY TIPS

The sophisticated spyware and digital attacks outlined in this report are used to target individuals who are of particular interest to government spyware operators because of their professional background, civil society work or information they possess. If you believe that you are at heightened risk of such attacks, there are practical steps you can take to make these kinds of advanced digital attacks more difficult:

- Update your web browser and mobile operating system software as soon as any security updates are made available for your devices.
- Enable the high security "Lockdown Mode" if you use an Apple device. This can make a successful compromise of your device more challenging for an attacker.
- Be wary of clicking links from strangers. Do not rely only on the preview of the URL displayed on messaging apps or social media platforms as that might be deceptive.
- Pay attention to any changes in devices' functioning (i.e., shortened battery life). However, this by itself is not a strong indicator of suspicious activity.
- Disable the 'Direct Messages from Anyone' option on X (formerly known as Twitter).
- On personal Facebook accounts, manage privacy settings to limit your profile's visibility to existing friends and evaluate any new friend or Messenger requests before accepting.
- If you receive a state-sponsored attacker warning you should seek expert help to understand any ongoing risks for your accounts or devices.

If you are a human rights defender, journalist, or member of civil society and believe you have been targeted by this campaign or have received similar attack links through social media, please go to https://securitylab.amnesty.org/contact-us/

[21] The Google Threat Analysis Group states that it is set up to "counter government-backed attacks". Google, Threat Analysis Group, https://blog.google/threat-analysis-group/ (accessed on 28 September 2023).

3. INTRODUCTION

Over the past decade, civil society organizations, researchers, and journalists have, through a steady stream of disclosures, exposed how governments around the world have been unlawfully targeting activists, journalists, and government officials using tools developed by private cyber-surveillance companies. Amnesty International and numerous civil society organizations have repeatedly warned that the opaque trade and deployment by states of privately manufactured surveillance technologies, particularly spyware, have wrought a digital surveillance crisis.[22] This crisis has severely and detrimentally impacted human rights, media freedoms, and social movements across the world. The 2021 Pegasus Project[23] disclosures – which exposed the global scale and breadth of unlawful surveillance facilitated by NSO Group's Pegasus spyware – and subsequent civil society research[24] has forced governments around the world to take note of the massive scale and breadth of spyware abuse, spurring the beginnings of action to rein in some of the most notorious spyware vendors and seeking accountability for the victims of unlawful surveillance.

Now, a new investigation coordinated by EIC media network with technical support from Amnesty International's Security Lab, has laid bare how government action has been inadequate and ineffective in ending spyware abuse.[25] The new Predator Files disclosures have exposed how states' use of privately manufactured spyware and surveillance tools continues to be out-of-control and threatening to individuals' human rights, as states and surveillance vendors continue the unchecked sale, transfer, and use of surveillance technologies across the world.[26]

The Predator Files disclosures show how a suite of highly invasive surveillance technologies supplied by Intellexa alliance – which is comprised of an alliance of surveillance vendors with corporate presence in European Union member states, as well as other countries around the world – is being sold and transferred around the world with impunity. The disclosures show the global scale and breadth of sales of surveillance technologies of this one alliance of vendors, which has been supplying its wares to Egypt, Libya, Madagascar, Saudi Arabia, Viet Nam, and France among many others between 2007 to 2022.[27] These transfers pose a high likelihood of human rights abuse due to past instances of unlawful surveillance in these countries and/or an absence of domestic surveillance safeguards that could prevent these technologies from being unlawfully unleashed on civil society, journalists, or opposition politicians.

In this report, Amnesty International's Security Lab has also uncovered a previously undisclosed targeted spyware operation using Intellexa's Predator spyware product with targeting aligned with government interests of Viet Nam. The surveillance campaign targeted at least 50 social media accounts belonging to 27

---

[22] Amnesty International, *Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector* (Index: DOC 10/4491/2021), 23 July 2021, https://www.amnesty.org/en/documents/doc10/4491/2021/en/; Amnesty International, *Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology* (Index: DOC 10/4516/2021), 27 July 2021, https://www.amnesty.org/en/documents/doc10/4516/2021/en/

[23] The Pegasus Project was a ground-breaking collaboration by more than 80 journalists from 17 media organizations in 10 countries coordinated by Forbidden Stories, a Paris-based media non-profit, with the technical support of Amnesty International.

[24] See, for example, Access Now, "Spyware in warfare: Access Now documents first-time use of Pegasus tech in Azerbaijan-Armenia conflict", 25 May 2023, https://www.accessnow.org/press-release/spyware-warfare-pegasus-in-azerbaijan-armenia-conflict/; Citizen Lab, "Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware", 12 January 2022, https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/

[25] The full EIC reporting on the Predator Files is published simultaneously to this report. Links to the reporting can be found at EIC, Projects, https://eic.network/#projects

[26] EIC, Projects, https://eic.network/#projects

[27] EIC, Projects, https://eic.network/#projects

individuals and 23 institutions around the world with "1-click" spyware infection links connected to Intellexa's Predator spyware attack infrastructure. Those targeted include senior political figures in the European Parliament, the European Commission, and EU-based journalists, academic researchers, and think-tanks. In addition to these, other attempted targets include United Nations officials, the President of Taiwan, United States Senators and Representatives, and other diplomatic authorities. The targeting of these individuals occurred as recently as June 2023. Amnesty International has also identified shipment records and trade data and, for this report, draws on research by EIC partners into sales of the Intellexa alliance's surveillance and infection solutions. This research reveals that the tools were sold through various Vietnamese broker companies to a government end-user, the Vietnamese Ministry of Public Security. Amnesty International has not forensically identified any successful infections from this campaign, however the known capabilities of the Predator spyware system, in addition to the brazenness, and at times carelessness of this surveillance operation demonstrate the enormous risks posed by the unchecked proliferation and transfers of these tools.

Amnesty International's analysis of recent technical infrastructure linked to the Predator spyware system indicates likely active customers or targeting of individuals in Sudan, Madagascar, Kazakhstan, Mongolia, Egypt, Indonesia, Vietnam, and Angola among others. This builds upon the 2021 research from Citizen Lab and Meta, who documented suspected Predator customers active in Saudi Arabia, Oman, Greece, Serbia, Trinidad and Tobago, Armenia, Egypt, Colombia, Côte d'Ivoire, Viet Nam, the Philippines, Germany, Indonesia, and Madagascar.[28]

By analysing marketing material accessed by EIC, Amnesty international has been able to ascertain the technical capabilities of a suite of surveillance products that were developed, operated, and marketed between 2007 to 2022 by the constituent companies of what became the Intellexa alliance.[29] These include a host of targeted and mass surveillance technologies. Targeted surveillance technologies include highly invasive mobile spyware like Predator, which can be delivered to devices using either 1-click attacks or 0-click attacks. The Predator spyware was originally developed by the North Macedonian surveillance company Cytrox, which is part of the Intellexa group of companies (see Table 1, Summary of Companies).

Disclosures as part of the Predator Files investigation also document various "vectors" or techniques offered by the Intellexa alliance to install the spyware through "tactical attacks", which enable the targeting of devices in close physical proximity, using multiple types of network injection methods and attacks against mobile phone basebands. In addition, strategic infection methods have also been developed, operated, and marketed by the Intellexa alliance. Strategic infection systems allow a state actor to deliver silent infection attempts to target users at cooperating internet service providers, or across a whole country if the spyware operator has direct access to internet traffic. Strategic infection systems resemble mass surveillance tools as they require access to large-scale internet traffic to target and infect individuals. The mass and "massive" surveillance products offered by the Intellexa alliance suggest an evolution of earlier surveillance technologies from lawful interception systems that allowed traffic monitoring in a targeted, individualised manner – that potentially allowed for more checks and limitations- to more overbroad and indiscriminate methods.[30] Both of these types of surveillance – namely, highly invasive spyware and indiscriminate mass surveillance tools – are fundamentally incompatible with human rights.

These findings are just the tip of the iceberg. As surveillance companies and their state clients continue to hide behind the rhetoric of national security and confidentiality to evade transparency and accountability, the actual scale and breadth of unlawful targeting using tools supplied by the Intellexa alliance is likely to be much higher. Warnings by civil society and lessons from the Pegasus Project mean that for each of the countries where disclosures reveal that the Intellexa alliance has sold its technologies, civil society targeting could be taking place unchecked and with impunity at a massive scale. These new disclosures make clear, yet again, that unchecked sale and transfer of surveillance technologies could continue to facilitate human rights abuse at a global scale, as companies are still being allowed to freely sell and transfer their wares in

[28] Meta, *Threat Report on the Surveillance-for-Hire Industry,* 16 December 2021, https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf; Citizen Lab, "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware", 16 December 2021, https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

[29] Amnesty International, 6 October 2023, https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/

[30] Wiki Leaks, Amesys product descriptions document for the Prague ISS World Europe 2008 Conference, https://wikileaks.org/spyfiles/files/0/21_200810-ISS-PRG-AMESYS.pdf (accessed on 26 September 2023).

secrecy. New evidence of unlawful targeting shows yet again that any claims by companies that unlawful targeting are anomalous are decidedly false.[31] Human rights abuse is a feature of the industry, not a bug.[32]

Civil society has long warned that a culture of impunity specific to targeted digital surveillance has developed that must be urgently countered. The steady stream of disclosures by civil society should have spurred more meaningful action from governments at a national, regional, and multi-lateral level. While some steps have certainly been taken in the right direction, civil society, journalists and researchers continue to lead on exposing this clandestine industry and unaccountable sphere of state practice, through hard-won insights.[33]

Amnesty International previously cautioned that civil society disclosures should not be the only form of check on states and surveillance companies.[34] The continuing trade in surveillance technologies, and its abuse exposed through these latest disclosures, must spur further urgent and concerted action by states. States must demonstrate leadership to end human rights abuses resulting from the unlawful use of targeted surveillance technologies and ensure that meaningful avenues for accountability are available to victims of abuses.

[31] Amnesty International, *Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology* (previously cited), https://www.amnesty.org/en/documents/doc10/4516/2021/en/
[32] Amnesty International, *Operating in the shadows: Investor risk from the private surveillance industry* (Index: DOC 10/4359/2021), 21 October 2021, https://www.amnesty.org/en/documents/doc10/4359/2021/en/
[33] Amnesty International, *Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology* (previously cited), https://www.amnesty.org/en/documents/doc10/4516/2021/en/
[34] Amnesty International, *Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector* (previously cited) https://www.amnesty.org/en/documents/doc10/4491/2021/en/

4. THE INTELLEXA ALLIANCE AND PREDATOR SPYWARE

This chapter summarises the Intellexa alliance's track record in selling surveillance technologies around the world. Despite repeated reporting on cases of abuse of their tools to unlawfully target individuals and organisations, our findings show once again the inadequacy of safeguards designed to prevent these types of abuses, including within the EU. The chapter then outlines how Intellexa's Predator spyware can be used to infect devices, drawing on brochures and technical documents obtained by EIC, demonstrating how this technology is inherently human rights abusive.

The majority of the chapter focuses on a case discovered by Amnesty International's Security Lab where Intellexa's Predator spyware was used to target diverse subjects. This case study provides insight into how an operator of Intellexa spyware can target individuals and institutional accounts in an attempt to infect their devices, as illustrated by a recent campaign targeting a journalist from Viet Nam, and civil society as well as EU, US and other political leaders working on issues of interest to the government of Viet Nam. Amnesty International's Security Lab has not confirmed any cases of successful infection related to this case study, but the case study does demonstrate the potential for one operator to target individuals and organisations around the world with a highly invasive form of spyware. The chapter concludes with Amnesty International's assessment of responsibility for this use of Predator spyware.

4.1 A HISTORY OF SURVEILLANCE ABUSES

The Intellexa group advertises itself as an "EU based and regulated company".[35] The annual financial documents of Intellexa's parent company, Thalestris Ltd., state that Intellexa's principal activity is to "provide intelligence products for law enforcement agencies.[36] The Intellexa alliance reportedly comprises Nexa Technologies and Advanced Middle East Systems (Nexa group), and WiSpear, Cytrox and Senpai Technologies (Intellexa group).[37] The Nexa and Intellexa groups of companies control multiple corporate entities, some of which have been renamed. The entities span various jurisdictions, both within and outside

[35] Intellexa, https://web.archive.org/web/20230719063910/https://intellexa.com/ (accessed on 19 July 2023).
[36] Thalestris Limited, "Annual report and consolidated financial statements for December 2021", p.29, (accessed in August 2023).
[37] Nexa Technologies, "Intellexa Alliance: Intellexa, The Intelligence Alliance, to Provide Unmatched End-To-End Intelligence Solutions for Law Enforcement and Intelligence Agencies", 16 February 2019, https://web.archive.org/web/20200109072024/https://www.nexatech.fr/intellexa-alliance-press-news; Fast Company, "Inside the shadowy world of spyware makers that target activists and dissidents", 26 June 2019, https://www.fastcompany.com/90369108/inside-the-shadowy-world-of-spyware-makers-that-target-activists-and-dissidents

the EU. These countries include Greece, Ireland, France, Germany, the Czech Republic, Cyprus, Hungary, North Macedonia, Switzerland, Israel and the United Arab Emirates (UAE).[38]

The entities and countries listed here are a non-exhaustive accounting of the corporate presence of the Intellexa alliance. The exact nature of links between these companies are shrouded in secrecy, as corporate entities and the structures between them are constantly morphing, renaming, rebranding, and evolving. As in the case of other spyware vendors like the notorious NSO Group, the opaque and unendingly complex corporate structures make it easier for companies who seek to evade accountability, transparency, and government regulation, including regional and national export control and corporate due diligence mechanisms.[39] In the case of the Intellexa alliance, the picture is even more complex, due to corporate structures of not only one primary company, but allied surveillance product vendors, parent companies, and their investors. All of which make the complete picture even more complex and opaque, which renders accountability and transparency for unlawful targeting using tools of this surveillance alliance even more difficult.

These disclosures are far from the first time that the companies in the Intellexa alliance have been linked to human rights abuse around the world. In 2011, the International Federation for Human Rights (FIDH) and The League of Human Rights (LDH) filed a criminal complaint against Amesys for complicity in acts of torture over sales of surveillance technology to Libya that took place in 2007.[40]

LDH and FIDH filed a second complaint in 2017 regarding the sale of the same technology to Egypt by Nexa Technologies in 2014, which led the French justice to open a second criminal probe for complicity in torture and enforced disappearance against Nexa[41]. Nexa Technologies and several of its executives have been formally indicted regarding this second probe in 2021, but the indictments were cancelled one year later by the Paris court of appeal.[42] Nexa is one of the companies that forms part of the Intellexa alliance.

In 2021, Citizen Lab found that an exiled politician and a journalist from Egypt were hacked with Predator spyware.[43] In 2022, a series of investigations and disclosures revealed that Greek journalist Thanasis Koukakis, and the leader of an opposition party in Greece and a sitting Member of European Parliament, Nikos Androulakis, were targeted with Predator and wiretapped by the Greek National Intelligence Service (NIS).[44] A newspaper also published a list of high-profile individuals allegedly under state surveillance and/or targeted with Predator.[45] In 2023, it was revealed that a Meta executive of US-Greek nationality was targeted

---

[38] U.S. Department of State, "The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities" ,18 July 2023, https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities-2/; European Parliament, Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation) 15 June 2023, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.pdf; Citizen Lab, "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware" (previously cited), https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/; https://www.business-humanrights.org/de/unternehmen/nexa-technologies/CRFS, Nexa Technologies https://www.crfs.com/partner/nexa-technologies/ (accessed 26 September 2023); Intelligence Online, *France's Nexa acquires European interception specialist Trovicor*, 3 December 2019, https://www.intelligenceonline.com/surveillance--interception/2019/12/03/france-s-nexa-acquires-european-interception-specialist-trovicor,108384645-art, 3 December 2019, https://www.intelligenceonline.com/surveillance--interception/2019/12/03/france-s-nexa-acquires-european-interception-specialist-trovicor,108384645-art

[39] Amnesty International, *Operating from the Shadows: Inside NSO Group's Corporate Structure* (Index: DOC 10/4182/2021), 31 May 2021, https://www.amnesty.org/en/documents/doc10/4182/2021/en/

[40] International Federation for Human Rights, "FIDH and LDH file a complaint concerning the responsibility of the company AMESYS in relation to acts of torture", 19 October 2011, https://www.fidh.org/en/region/north-africa-middle-east/libya/FIDH-and-LDH-file-a-complaint

[41] International Federation for Human Rights, "Q/A Surveillance and torture in Egypt and Libya: Amesys and Nexa Technologies executives indicted", 22 June 2021, https://www.fidh.org/en/region/north-africa-middle-east/egypt/q-a-surveillance-and-torture-in-egypt-and-libya-amesys-and-nexa

[42] Tech Xplore, "Charges dropped against French company over Egypt spyware", 14 December 2022, https://techxplore.com/news/2022-12-french-company-egypt-spyware.html

[43] Citizen Lab, "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware", (previously cited), https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

[44] Inside Story, " Από τον Κουκάκη στον Ανδρουλάκη: Νέα τροπή στην υπόθεση του spyware Predator", 27 July 2022, https://insidestory.gr/article/apo-koykaki-androylaki-nea-tropi-ypothesi-predator; European Parliament, *Report of the 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)) , 22 May 2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf; Amnesty International, "Greece's surveillance scandal must shake us out of complacency", 26 January 2023, https://www.amnesty.org/en/latest/news/2023/01/greeces-surveillance-scandal-must-shake-us-out-of-complacency/

[45] Documento, "Αποκάλυψη: Αυτούς παρακολουθούσε – Αυτή την Κυριακή στο Documento", 5 November 2022, https://www.documentonews.gr/article/apokalypsi-aytoys-parakoloythoyse-ayti-tin-kyriaki-sto-documento/ ; Economist, "Fresh allegations in a Greek phone-hacking scandal", 10 November 2022, https://www.economist.com/europe/2022/11/10/fresh-allegations-in-a-greek-phone-hacking-scandal

with Predator and reportedly wiretapped by NIS.[46] An investigation by Greece's privacy watchdog (the Hellenic Data Protection Authority) on the use of Predator traced 350 SMS messages attempting to install surveillance software and found 92 'targets'.[47]

In September 2023, Citizen Lab revealed that between that a former Egyptian Member of Parliament was targeted with the Predator spyware.[48]

In July 2023, the US Government's Bureau of Industry and Security placed four corporate entities within the Intellexa alliance on its entity list for malicious cyber activities stating that the companies "engaged in trafficking in cyber exploits used to gain access to information systems, threatening the privacy and security of individuals and organizations worldwide".[49] The corporate entities included on the list are Intellexa S.A. in Greece, Intellexa Limited in Ireland, Cytrox AD in North Macedonia, and Cytrox Holdings Crt in Hungary.

Given that companies in the Nexa group and the Intellexa group's own corporate entities have been suspected of human rights abuses previously in Greece, Egypt, and Libya, Amnesty International wrote to the companies asking them what steps they took since the publication of these first disclosures to ensure they are operating in a rights-respecting manner in line with the UN Guiding Principles, and what steps they took to provide remedy to those affected. Amnesty International did not receive a response at the time of publication. However, former Nexa group executives sent a response to EIC partners on behalf of their companies including Nexa Technologies and Advanced Middle East Systems. They stated that (translated from French by Amnesty International):

> "We have never underestimated the ethical dilemma posed by our work. We were aware that some of the countries with whom we were able to establish commercial relationships were far from perfect in terms of the rule of law. But we were just as mindful of the fact that our approach was most often part of an effort by the international community to help these countries move towards democracy.
>
> "By sharing the moral and very concrete dilemmas that we have had to face during our professional life, we have just mentioned the role of the authorities and in particular the French authorities, when it comes to the export of a French solution. In several of the disputed countries that you mention, we have not only obtained export authorization, but also have simply taken the path of close cooperation initiated by France with these same countries."

Their response continued:

> "French companies must be able to operate within a clear regulatory framework.
>
> "We trusted the authorities to give us the green light. Since then, starting in 2021, we have been trying to move forward with the help of external support, in order to better understand the reality on the ground in different countries, and to be able to assess the risks of violations of fundamental rights. We thus established a process, which includes people external to the company who are specialized in human rights.
>
> "Following their opinion, we made the decision to cease all commercial relationships with a State. Over the past two years, we have also refused to enter into commercial relationships with several other States."

Regarding compliance with export control regulations, they further stated:

> "As we explained above, all the marketing contracts by the companies you name scrupulously complied with export regulations.
>
> "As we explained in the introduction, when we obtain authorization from the SBDU, we considered in good faith that our product could be exported legally. This was all the more true for a country like

---

[46] New York Times, "Meta Manager Was Hacked With Spyware and Wiretapped in Greece", 20 March 2023, https://www.nytimes.com/2023/03/20/world/europe/greece-spyware-hacking-meta.html; *European Parliament, Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware* (previously cited), https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.pdf

[47] Euroactiv, "Privacy watchdog finds 92 'targets' in Greek wiretapping scandal", 21 July 2023, https://www.euractiv.com/section/politics/news/privacy-watchdog-finds-92-targets-in-greek-wiretapping-scandal/

[48] Citizen Lab, "Predator in the Wires: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions", 22 September 2023, https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/

[49] U.S. Department of State, "The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities" (previously cited), https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities-2/

> Egypt, with which the French authorities exalted their intense cooperation, and on whose territory our own security [security of France] was also at stake. This is precisely one of the reasons why the Paris Court of Appeal annulled our indictments in December 2022, as reported in the press.
>
> "Contrary to what you think, the place of registration of our companies was never intended to circumvent regulations. It was based on a business logic because our clients often required a local presence."

In response to EIC about sales of Predator, their response also states that:

> "We denounced these contracts [including with Vietnam] after the 2021 judicial search, which made us become aware of the risks related to these deals. We realized that the authorizations granted did not sufficiently protect us and did not constitute any guarantee against human rights violations."

Given the nature of the spyware industry and its capability to facilitate human rights abuse, alongside the Intellexa alliance's own knowledge of previous instances of abuse, the alliance of surveillance companies knew, or ought to have reasonably known that human rights abuse could occur. In addition, given the history of human rights abuse detailed in this section, export authorities and other state authorities had ample warning of the likelihood that sales of Intellexa alliance products posed serious human rights risks.

4.2 INTELLEXA'S PREDATOR SPYWARE

Intellexa's Predator spyware system is a form of highly invasive spyware that by default gains total access to all data stored or transmitted from the target's device, and which is designed to leave no traces on the target device, to render any independent audit of potential abuses impossible. As such Predator is fundamentally incompatible with human rights and should be banned.

Amnesty International's Security Lab's analysis of brochures and technical documents provided by EIC provides new insight into how this spyware functions on a technical level and the methods by which it infects targets' devices.

According to these documents, Predator spyware infections are managed via a web-based system which Intellexa terms the "Cyber Operation Platform". The Predator interface allows the spyware operator to initiate infection attempts against a target phone, and if successful to retrieve and access sensitive information including photos, location data, chat messages and recordings from the infected device.

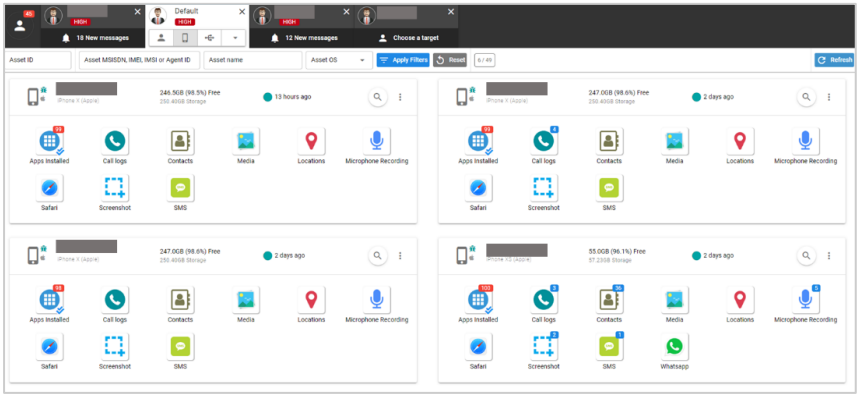


Figure 1: Intellexa Predator spyware interface (source: EIC documents)

The full Predator system includes a number of distinct software and infrastructure components. These include the spyware agent itself, which is installed on the target's device, and the software exploits and attack vectors necessary to install the spyware covertly on the target phone. The company has used a number of marketing terms to describe their mobile spyware products including Green Arrow for their Android spyware agent, Red Arrow for their iOS spyware agent, Predator, Helios, and NOVA among others. In this report we refer to this overall mobile spyware product as Predator as we believe all these product names refer to the same set of broadly related spyware technology originally developed by Cytrox and which continues to be developed, marketed and sold by the Intellexa alliance.

The exploit code and spyware payloads are delivered to a target device from what Intellexa terms their "installation server". Once a phone is infected with the Predator agent, it connects to a command and control (CNC) network where the operators can issue commands to the agent, such as to retrieve certain files or to activate the microphone. Commands are sent to the device via an anonymisation network which aims to obscure the location and identity of the spyware operator and make it more difficult for researchers to identify the source and nature of the attacks. The "installation server" and CNC servers must be publicly accessible on the internet to allow connections from targeted devices. Other servers including the anonymisation network and the "Cyber Operations Core" may be firewalled or isolated inside the network of the Predator customer.

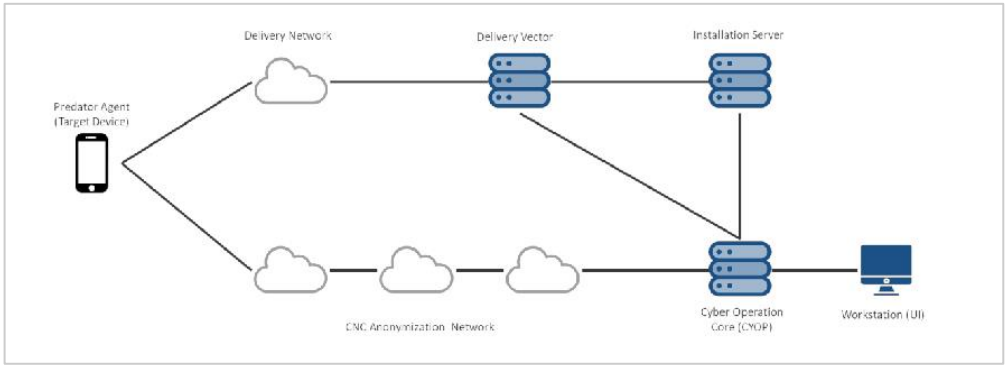


Figure 2: Predator high-level server architecture (source: EIC documents)

Various "1-click" and "zero-click" infection vectors can be used to target and infect a particular device. Previous publicly documented attacks linked to Predator were delivered through social engineering messages containing malicious URL which are known as a 1-click attacks.[50] The success of 1-click spyware attacks depends on the ability of the spyware operator to create trust with the target, and to customize the attack URL and the message in way which is enticing for the target to open the link. In this report we will focus on "1-click" attacks which we also identified being used in the attacks described in the next section of this report.[51]

If the targeted phone is running a supported browser and operating system version, an exploit chain will be served which first compromises the web browser before attempting to escalate privileges and install the full spyware agent on this device. Such "1-click" attacks are particularly powerful as they can be used to successfully target a vulnerable device anywhere in the world just by opening a link.

4.3 PREDATOR CASE STUDY: @JOSEPH_GORDON16

In April 2023, Amnesty International's Security Lab identified a Twitter (now X) account with the username @Joseph_Gordon16 sharing links publicly containing Intellexa Predator infection links. The account was first identified from online searches for active Intellexa domains which the Security Lab had identified through ongoing efforts to track Intellexa spyware infrastructure.

Over a two-month period after identifying the attacker's account, Amnesty International's Security Lab observed dozens of instances where the "@Joseph_Gordon16" account sent public tweets and replies to tweets by other users that contained links to malicious custom URL shorteners and spoofed news website URLs. Amnesty International was able to match these links to known Intellexa Predator domains uncovered during earlier research. Specifically, two domains Inktonews[.]co, and witteridea[.]co, both of which were tweeted by the "@Joseph_Gordon16" account, were previously identified in Security Lab research as active

[50] Citizen Lab, "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware" (previously cited), https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/; Inside Story, "Predatorgate: Τι έγραφαν τα SMS-παγίδα που έλαβαν επιχειρηματίες, υπουργοί και δημοσιογράφοι", 27 July 2023, https://insidestory.gr/article/predatorgate-ti-egrafan-ta-sms-pagida-poy-elavan-epiheirimaties-ypoyrgoi-kai-dimosiografoi

[51] Such infection URLs are also often time-limited and geographically-restricted to make it more difficult for researchers to fully analyse the attack links or capture samples of the highly valuable zero-day exploit used to infect fully updated devices.

Predator URL shortener domains. Spyware 1-click and URL shortener domains are often registered with deceptive names, with the aim of tricking a target into believing the link is legitimate. One of the domains "Inktonews[.]co", suggests that the link forwards to a news article. The second domain "witteridea[.]co" is intended to mimic a link related to the Twitter/X platform.

Figure 3: Screenshot of "@Joseph_Gordon16" account

Following Amnesty International's discovery of the initial attack tweets, the @Joseph_Gordon16 account continued to tweet suspicious links for newly established domains including asean-news[.]net, southchinapost[.]net, and caavn[.]org. Both asean-news[.]net and southchinapost[.]net matched patterns associated with known Predator servers.

Amnesty International shared a subset of this activity with other security researchers, including analysts at Google's Threat Analysis Group which has a history of tracking attacks and exploit campaigns carried out by the Intellexa alliance and other commercial surveillance vendors.[52] The Threat Analysis Group confirmed to Amnesty International that Google's own research had identified that the domains and URLs shared by the @Joseph_Gordon16 account including southchinapost[.]net, Inktonews[.]co, and witteridea[.]co are part of Intellexa's Predator spyware system.

Researchers at Google's Threat Analysis Group also successfully accessed the Predator infection URLs tweeted by the @Joseph_Gorden16 account while it was still active. The original malicious URL shortener link hosted at southchinapost[.]net redirected to a Predator installation server at scanningandinfo[.]online. In this instance the installation server did not attempt to serve an exploit or infect the test device.

PURPOSE	URL
URL Shortener Landing Page	https://southchinapost[.]net/eNISDKnI
Predator Installation Server	https://scanningandinfo[.]online/jbz7xv9xox0bn2ya3gat39i64/xfer-ovc?sip=2d2c3a697858f315177940709c236a69
Predator Installation Server	https://scanningandinfo[.]online/jbz7xv9xox0bn2ya3gat39i64/xfer-ovc?r=true&sip=2d2c3a697858f315177940709c236a69

Table 2: Example redirect chain from Predator link shared by @Joseph_Gordon16

A third domain caavn[.]org, shared by the X account @Joseph_Gordon16 was no longer online at the time of analysis which prevented us from determining if it matched the fingerprint of Intellexa servers. The caavn[.]org domain was previously hosted at IP address 212.90.121.247, which also hosted two more

[52] Google's Threat Analysis Group, "Protecting Android users from 0-Day attacks", 19 May 2022, https://blog.google/threat-analysis-group/protecting-android-users-from-0-day-attacks/

domains imitating legitimate Vietnamese websites xuatnhapcanhvn[.]info and tokhaiytehanoi[.]org.[53] The appearance of multiple Viet Nam related domain names on the same internet server, around the same time period, and registered from the same internet provider suggest that all three domains were registered by the same operator.

Figure 4: Attacker-controlled caavn[.]org domain imitating a news article from the South China Morning Post

Unlike the URL shortener domains described earlier, the caavn[.]org tweet contained a full URL which was similar to an original news articles published by the South China Morning Post newspaper. The approach of mirroring a legitimate news article or web page may be another attack technique used by the attackers to entice the target to open the link. The link preview shown by X matches the authentic newspaper domain of the South China Morning Post on scmp.com, suggesting the attackers had configured their malicious link to redirect to the South China Morning Post as a decoy website to display when accessed by the X link preview generator (see Figure 4).

The fact that some of the Intellexa domains used in the attacks were designed to imitate legitimate Vietnamese websites suggests a connection with Viet Nam-linked actors which is supported by significant circumstantial evidence based on an analysis of the attacker's X account and the background of the targets. The first tweet from the account, in 2020, is in Vietnamese. The account later sends other tweets containing an attacker-controlled domain name to Thời Báo, a German-based Vietnamese news outlet as described in more detail in 3.4.1 below.

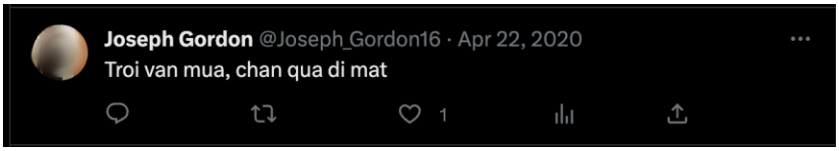


Figure 5: Early tweet from @Joseph_Gordon16 written in Vietnamese.

4.4 @JOSEPH_GORDON16'S TARGETS

The wide-ranging and public spyware targeting attempts by the "@Joseph_Gordon16" X account provided Amnesty International's Security Lab with insight into the goals of the Intellexa Predator operator behind this attack campaign. The targets selected by this account included journalists, academic researchers working on security issues in the South China Sea and Vietnam, as well as senior political officials in the EU, US, and

[53] The domains names are visually similar to the official immigration department of the Viet Nam Ministry of Police (xuatnhapcanh.gov.vn) and a website used in Viet Nam to record health declarations during the COVID-19 pandemic (tokhaiyte.vn).

elsewhere, involved in work related to international fishing regulation, an issue of interest to the Vietnamese authorities (see section 4.4.2).

The following section will expand on a number the key cases of attempted targeting against journalists, civil society members and other public figures. While the range of targets is diverse, both in terms of profile and location, the targets are in many cases relevant to Vietnamese political, military and intelligence interests.

A full list of tweets can be found in Annex II of this report.

CATEGORY	NUMBER OF SPYWARE TARGETING ATTEMPTS
News media	16
Academia	2
Politicians/institutions	27
Think tanks	6
Other	7

Table 3: Example redirect chain from Predator link shared by @Joseph_Gordon16

4.4.1 TARGETING OF THOIBAO.DE

One of the earliest attack tweets sent by the "@Joseph_Gordon16" X account was targeted at a Berlin-based independent media website Thời Báo, which covers news about Viet Nam. The tweet was sent in reply to an article published by Thời Báo about a corruption investigation involving the Viet Nam Ministry of Defence. In the reply written in Vietnamese, the account operator suggests that the corruption investigation is related to infighting or a power struggle between the Viet Nam Ministry of Public Security and the military (Figure 6).

Figure 6: Attack tweet to Thoibao.de - Text: Công an đấu đá nội bộ, Bộ Công an bắt công an Hải Dương

The included link "lnktonews.co" may appear to be a link to a news website but is in fact a link to Predator infection infrastructure which appears attempted to infect individuals involved with this media organization with the Predator spyware.

DATE	TO	URL	PLATFORM
09-Feb-23	thoibao_de	https://lnktonews[.]co/MEmK	X

Table 4: Predator infection link sent to Thoibao.de on X

This attempt to target and infect a media organisation and its media workers based in the EU with spyware is a clear threat to the ability of journalists to report and publish openly on topics relevant to their audience

even in diaspora communities. The risk for journalistic sources who communicate with journalists who are later hacked can also be extremely severe.[54]

Khoa Lê Trung in his office.
© Amnesty International

KHOA LÊ TRUNG, EDITOR-IN-CHIEF, THOIBAO.DE

Khoa Lê Trung is a journalist from Viet Nam living in Berlin, Germany. He is the editor-in-chief of Thoibao.de. Thoibao.de's account was targeted with Intellexa's Predator spyware, sent as a 1-click attack over X.

Thoi Bao reports on political, economic, and environmental issues in Viet Nam and globally. Due to the repressive media landscape in the country, where those who express critical views online face an intense crackdown, the right to freely receive and impart information within Viet Nam is unduly restricted.[55] Khoa Lê Trung is attempting to counter this through Thoi Bao's reportage, to ensure access to accurate information to Vietnamese people. The website has 20 million visits per month and is one of the most viewed Vietnamese media platforms operating from exile.

Targeted surveillance of the kind detailed in this report is one of the many forms of reprisals that journalists increasingly face for their work in Viet Nam, and globally. Surveillance is often accompanied by intimidation, harassment, and censorship online. Thoi Bao's targeting through Intellexa's Predator spyware is just one in a series of examples of offline and online repression that Khoa Lê Trung has faced over the years.

"You can't just sell [surveillance technologies] to countries like Viet Nam… this Western software, Western hardware attacks Germany or European [countries] back. This also harms the freedom of the press and freedom of expression for the people here in Germany as well"

Khoa Lê Trung

[54] See, for example, Amnesty International, "Uzbekistan: Tentacles of mass surveillance spread across borders", 31 March 2017, https://www.amnesty.org/en/latest/news/2017/03/uzbekistan-tentacles-of-mass-surveillance-spread-across-borders/
[55] Amnesty International, *Viet Nam: Let us breathe! Censorship and criminalization of online expression in Viet Nam* (Index: ASA 41/3243/2020), 30 November 2020, https://www.amnesty.org/en/documents/asa41/3243/2020/en/

Due to his work at Thoi Bao, Khoa Lê Trung has received death threats and intimidation for merely exercising his right to freedom of expression. He told Amnesty International, "I also get threats, especially from Vietnamese people in Germany, there are also people who call me or send me text messages and threaten me... to cut off my head if I carry on like this. There are also people who come straight to my office and tell me, 'Don't go on with your reports because it's not good for you.'" Due to these threats, Khoa Lê Trung has been placed under police protection in Berlin since 2018.

While the protection makes him feel somewhat safer, it also means some degree of restriction on everyday activities. "Every time I go to an event, I have to consider whether it makes sense or not, and whether it's worth it, because I always have to report it to the police before I go there. In case anything happens at that event", he told Amnesty International.

The repression he faces extends to the online realm. Khoa Lê Trung has received threats, been the subject of smear campaigns online and has often been labelled a "traitor". He told Amnesty International that since 2017, when he reported on a politically sensitive story about the kidnapping of a Vietnamese businessman in Berlin and faced pressure from the Vietnamese embassy to take down the story, Thoi Bao's website has been blocked in Viet Nam. He further told Amnesty International that his own Facebook account has also been blocked in the country. He noted that he often faces censorship of his videos on social media. When news videos are taken down by social media companies at the request of authorities, recovering them takes time and effort. However, some are lost forever. "We have to do a lot to get it back," he told Amnesty International. "There are videos that I can recover, but there are also videos that cannot be recovered", he added.

The latest targeting using Intellexa's Predator spyware detailed in this report is not the first time that he has been targeted with cyber-attacks. He told Amnesty International that Thoi Bao's website was targeted with Distributed Denial of Service (DDoS) attacks (see Glossary), which caused the website to crash. The practice of targeting using malicious links over social media, as detailed in this report, is dangerous not just for him, but other journalists who work for Thoi Bao as well. Khoa Lê Trung told Amnesty International, "...there are also many comments in there that it would be dangerous if someone clicked on this comment on Thoibao.de, that the computer could then probably be infected and break or the data could be stolen. Very dangerous. That's why I have to be very careful, including for my website employees". As a result of these attacks, he has spent significant time and resources in ensuring the digital security and safety of his website, himself, and his employees. This is time and resources that could be spent instead on journalistic work and reportage.

Khoa Lê Trung told Amnesty International that targeted surveillance attacks have an extremely detrimental impact on journalists and bloggers in Viet Nam. He believes that authorities in Viet Nam are behind these attacks, who he says are investing heavily to carry out digital attacks against dissenters online, including against his news platform.

He told Amnesty International that governments in Europe have a responsibility to control the sale and transfer of surveillance technologies. "You can't just sell them [surveillance technologies] to countries like Viet Nam.....so that this Western software, Western hardware attacks Germany or European [countries] back. This also harms the freedom of the press and freedom of expression for the people here in Germany, as well," he told Amnesty International.

Amnesty International research has previously identified other suspected state-aligned spyware campaigns targeting Vietnamese activists and bloggers based in Germany. A February 2021 investigation found that blogger and pro-democracy activist Bui Thanh Hieu was targeted with Windows spyware at least four times between February 2018 and December 2019.[56] The prominent activist had been repeatedly harassed by Vietnamese authorities before he sought sanctuary in Germany, where he has lived since 2013. Another blogger within Viet Nam, who was not named due to security concerns, was targeted three times between July and November 2020. These previous spyware attackers targeting Vietnamese activists in Germany are linked to an attack group known in the cybersecurity industry as Ocean Lotus. Ocean Lotus has also been

[56] Amnesty International, "Click and Bait: Vietnamese Human Rights Defenders Targeted with Spyware Attacks", 24 February 2021, https://www.amnesty.org/en/latest/research/2021/02/click-and-bait-vietnamese-human-rights-defenders-targeted-with-spyware-attacks/

repeatedly identified by cyber security firms as targeting Vietnamese political dissidents, foreign governments and companies.[57]

4.4.2 AN INTEREST IN FISHERIES: TARGETING OF EUROPEAN UNION AND UNITED NATIONS OFFICIALS

A second category of individuals targeted by the @Joseph_Gordon16 X account include multiple academics and officials working on maritime issues with a particular emphasis on academic researchers and officials responsible for European Union (EU) and United Nations (UN) policies on illegal or undocumented fishing.

The EU's efforts to combat illegal fishing are covered by the Illegal, Unreported and Unregulated (IUU) fishing regulation. In October 2017, the European Commission issued a 'yellow card' warning to Viet Nam over insufficient action to fight illegal fishing. The warning invited Vietnamese authorities "to engage in a formal procedure of dialogue to resolve the identified issues and implement the Action plan".[58] The yellow card warning did not stop the import of fish and seafood products from Viet Nam to the EU but indicated that Viet Nam was at risk of being identified as a non-cooperating country.

On 16 May 2023, the @Joseph_Gordon16 account replied publicly to a Spanish academic whose work is focused on illegal fishing and poaching policy (though the academic does not work on issues related to Viet Nam). This tweet contained another Predator infection link, this time hosted at asean-news[.]net (see Figure 7). The tweet was written in Spanish and references directly the EU "Yellow Card" system: "¿Cuál es su solución para deshacerse de la tarjeta amarilla?" ("What is your solution to get rid of the yellow card?").

Figure 7: Attack tweet sent to Spanish academic researching fisheries policy.

Twice on 8 February 2023, the account sent attack links to Ms Charlina Vitcheva (@vitcheva_eu), Director-General of DG Maritime Affairs and Fisheries at the European Commission. Both tweets included an identical link infection link with the Predator domain witteridea[.]co and the message "How will this issue be resolved?". Maritime Affairs and Fisheries (DG MARE) is the European Commission directorate responsible for administering European Union IUU mechanisms including the Yellow Card system. One attack tweet was sent in reply to a public tweet (see Figure 8) from Charlina Vitcheva which mentioned multiple institutional and public accounts, including that of Pierre Karleskind (@Pierre_Ka), a French MEP who chairs the Committee on Fisheries of the European Parliament (see Figure 9). A reply to a tweet on X, such as the message sent by the attacker, is sent to all accounts mentioned in the original tweet. The full list of targeted accounts is listed in Table. The European Union Mission Ocean Waters X account was also targeted twice with two different links, on 9 February 2023 and again on 1 June 2023 (see Figure 10). The targeting of this academic and the direct reference to the EU Yellow Card in the attack message, plus the other EU officials and politician who focus on this issue, suggest that the topic is of direct interest to the operator behind this Predator infection campaign.

[57] Amnesty International, "Vietnamese activists targeted by notorious hacking group", 24 February 2021, https://www.amnesty.org/en/latest/press-release/2021/02/viet-nam-hacking-group-targets-activist/; Reuters, "Facebook tracks 'OceanLotus' hackers to IT firm in Vietnam", 11 December 2020, https://www.reuters.com/article/facebook-vietnam-cyber-idCAKBN28L03Y

[58] European Commission, "Commission warns Vietnam over insufficient action to fight illegal fishing", 23 October 2017, https://ec.europa.eu/commission/presscorner/detail/en/IP_17_4064

Figure 8: Attacker replied to tweet from @vitcheva_eu on fisheries mentioning other accounts.

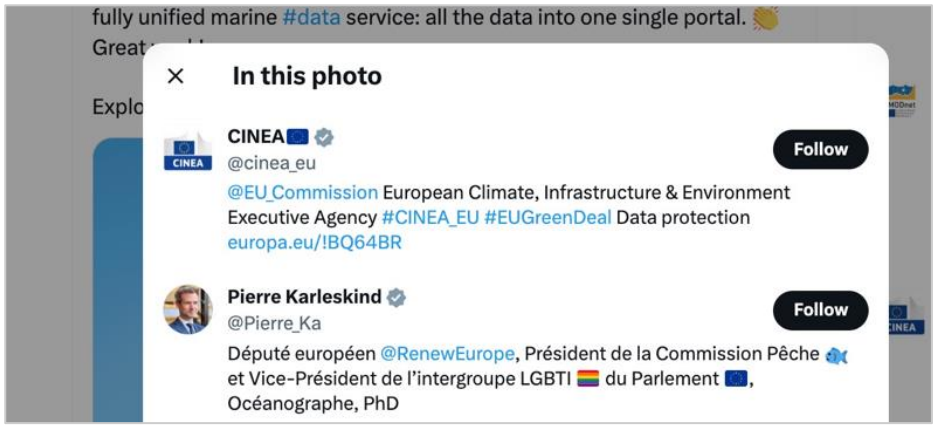


Figure 9: Account @Pierre_Ka mentioned in original tweet by @vitcheva_eu and included in attack reply.

Figure 10: Predator attack link sent on 1 June 2023

4.4.3 OTHER TARGETING OF INSTITUTIONS AND OFFICIALS

This research also identified attacks by @Joseph_Gordon16 on other EU officials and 11 institutions that are tied to the EU (including the "Mission Ocean Waters" attacks described above in 3.4.2).

Notably, the public X account of the President of the European Parliament, Roberta Metsola was targeted by "@Joseph_Gordon16" on 1 June 2023 with the southchinapost[.]net Predator infection domain.

Figure 11: Attack link sent to Roberta Metsola, President of the European Parliament.

Around the same time, the official institutional X account of the European Commission was also targeted by @Joseph_Gordon16 using the same Predator link sent to Roberta Metsola.

Figure 12: Attack link sent to official European Commission X account.

The X account of the German ambassador to the United States was also targeted by the "@Joseph_Gordon16" account on the 8 March 2023.

Figure 13: Attack link sent to Emily Haber, German Ambassador to the United States at time of targeting.

DATE	TO	URL	PLATFORM
08-Feb-23	@vitcheva_eu @EMODnet @cinea_eu @Pierre_Ka @EUgreenresearch @CMEMS_EU @FSUMDC @UNDPOceanInnov @REA_research @EU_ENV @EUClimateAction @eumissionocean	https://witteridea[.]co/LFJeZQu	X (formerly Twitter)
08-Feb-23	vitcheva_eu	https://witteridea[.]co/LFJeZQu	X
08-Mar-23	GermanAmbUSA	https://Inktonews[.]co/CVgp	X
01-Jun-23	EP_President	https://southchinapost[.]net/VuAfn	X
01-Jun-23	EU_Commission	https://southchinapost[.]net/VuAfn	X
01-Jun-23	EU_Commission	https://southchinapost[.]net/VuAfn	X
01-Jun-23	eumissionocean	https://southchinapost[.]net/VuAfn	X

Table 5: Attack links sent to EU political figures and EU institutions.

TARGETING OF STATE OFFICIALS IN THE US AND TAIWAN

The operator behind the '@Joseph_Gordon16' account tweeted an attack link at Tsai Ing-Wen, the President of Taiwan on 14 April 2023. A United States (U.S.) Senator for North Dakota, John Hoeven (@SenJohnHoeven), was also tagged in the original tweet by Tsai Ing-Wen. As a result, the reply tweet and attack link were also indirectly sent to the Senator's X account (Figure 14).

Figure 14: Attack link sent to Tsai Ing-wen (@iingwen) and U.S. Senator John Hoeven

The attacker-controlled website at caavn[.]org was likely configured to redirect link preview requests from X to the legitimate South China Morning Post website in order to create a realistic link preview. This is a common tactic used to infect devices with spyware. In this case, the preview contains information from a legitimate article published on the South China Morning Post website about security cooperation between the U.S. and Taiwan.

On the same date '@Joseph_Gordon16' also tweeted an attack link at the X account of the Ministry of Foreign Affairs of Taiwan. As '@Joseph_Gordon16' was replying to a tweet that originally tagged a U.S representative, Rep. Michael McCaul representing the Texas 10th district, the Representative would also have received the attack message automatically. Rep. McCaul was mentioned in the original tweet in his role as Chair of the House Foreign Affairs Committee in the U.S. Congress.

Figure 15: Attack link sent to the Ministry of Foreign Affairs of Taiwan and Rep. Michael McCaul.

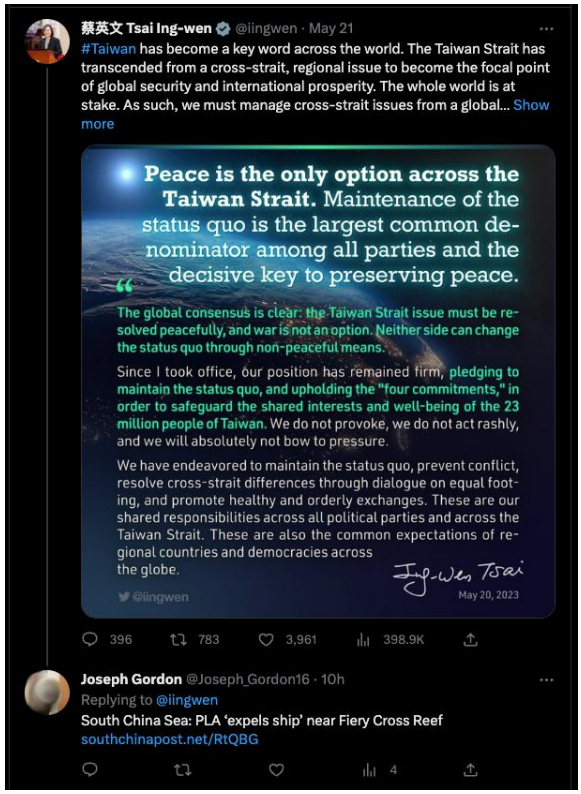


Figure 16: Attack link sent to Tsai Ing-wen (@iingwen) using new southchinapost[.]net Predator infection domain.

The '@Joseph_Gordon16' operator returned to target Tsai Ing-Wen once more time on 21 May 2023. The southchinapost[.]net Predator infection domain was used in this attack attempt (Figure 16).

SENIOR U.S. AND TAIWAN OFFICIALS AND INSTITUTIONS TARGETED WITH PREDATOR SPYWARE

DATE	TO	URL	PLATFORM
14-Apr-23	@iingwen @SenJohnHoeven	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14-Apr-23	@MofaTaiwan	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
22-May-23	@iingwen	https://southchinapost[.]net/RtQBG	X

Table 6: Attack links sent to U.S and Taiwan officials and institutions.

4.4.4 OTHER PREDATOR SPYWARE ATTACK ATTEMPTS LINKED TO THIS OPERATOR

In addition to the "@Joseph_Gordon16" X account, Amnesty International has identified another social media account which also sent links containing the same spyware domains. An account on Facebook "Anh Tran" shared additional Predator links containing the caavn[.]org domain. The use of the same custom domain name in links from both accounts confirms that both social media accounts are likely related to the same Predator operator.

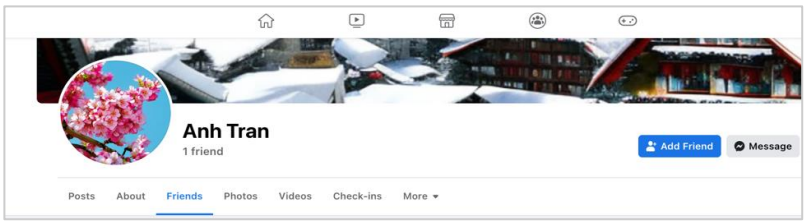


Figure 18: Facebook profile of the "Anh Tran" account

Amnesty International observed this account posting two public comments in March 2023 on the public Facebook page of a Vietnamese opposition political group "Liên Minh Dân Tộc Việt Nam", which is located in the U.S.[59] The attack links were posted publicly in Facebook comments and in this case imitated articles posted on the Vietnamese language "Tiếng Dân" news website (see Figure 19).[60] The "Tieng Dan" website has previously experienced Distributed Denial of Service (DDoS) attacks and has been targeted by the Ocean Lotus group.[61]

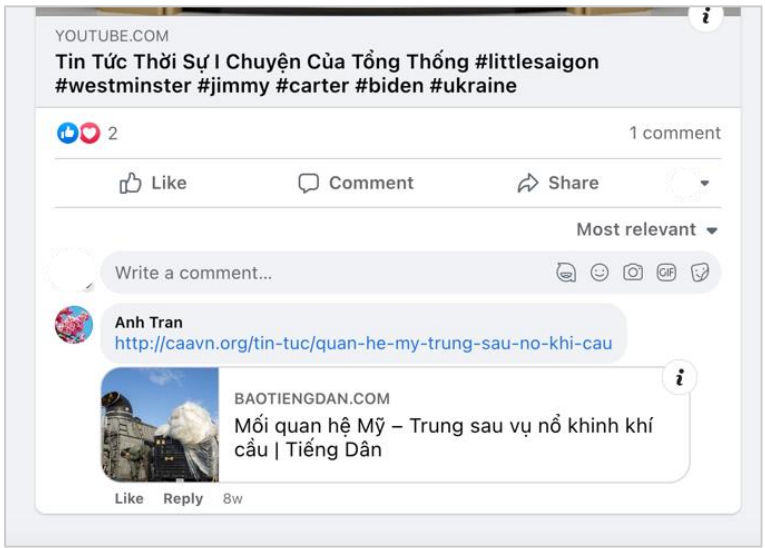


Figure 19: Attack link imitating baotiengdan.com

The additional attack targeting a Vietnamese diaspora political group on Facebook show the ongoing focus of the Predator operator behind these attacks. These publicly shared attack links likely represent only a subset of the overall targeting tied to this surveillance campaign. Additional attack attempts sent over instant messaging apps or through direct messages are more difficult for researchers to identify.

[59] Facebook, Liên Minh Dân Tộc Việt Nam, https://www.facebook.com/LMDTVN/ (accessed on 26 September 2023)
[60] Tiếng Dân, https://baotiengdan.com/ (accessed on 26 September 2023)
[61] Deflect, "News From Deflect Labs: DDoS attacks against Vietnamese Civil Society", 7 September 2018, https://deflect.ca/ddos-attacks-vietnamese-civil-society/

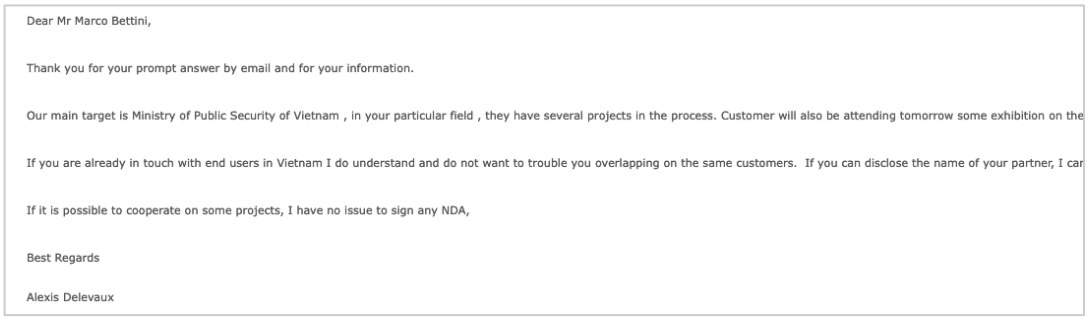
4.5 INTELLEXA ALLIANCE SALES TO VIETNAM

Amnesty International has additionally reviewed reporting and analysis prepared by EIC media partners based on confidential business records available to the media organisations as part of the "Predator Files" investigation. This reporting, shared with Amnesty International in advance of publication, describes sales of surveillance technologies from Intellexa alliance entities to the Vietnamese authorities. Taken together with the forensic and technical evidence outlined in Section 3.4, these findings by EIC partners, including Mediapart and Der Spiegel, further strengthen the technical evidence regarding the origin of the attacks.

Reporting by EIC describes that Nexa Technologies signed a deal for "infection solutions" with Viet Nam's Ministry of Public Security (MOPS) in early 2020 through the Nexa group's UAE-based sales subsidiary Advanced Middle East Systems. Their analysis also shows that the project, code named "Angler Fish" was offered with a two-year license and was worth 5.6 million euros. A second Nexa Technologies document, seen by EIC, dated January 2021 states that expected revenue regarding this contract was 3.36 million euros in 2021 and 2.44 million euros in 2022.

The reporting also identified another sales forecast record dated 26 January 2021, showing that Advanced Middle East Systems was trying to obtain an "extension" of the contract with Viet Nam's MOPS, worth 800,000 euros for "Blue Arrow". Intellexa alliance entities have used the "Arrow" branding including "Green Arrow" and "Red Arrow" as marketing names for their Predator spyware solutions. The documents available to EIC do not confirm if this contract extension was signed.

According to further records accessed by EIC, one month later, on 19 February 2021, Advanced Middle East Systems sold the Arrow spyware to the company Delsons Hong Kong Limited, registered in Hong Kong. Public records from the Hong Kong registry of companies[62] shows that Delsons Hong Kong is owned by Alexis Delevaux, a Swiss businessman living in Asia, who also serves as Monaco's Honorary Consul in Hanoi. A public leak of emails from spyware vendor Hacking Team includes emails from Mr. Delevaux in 2011 in which he expresses interest in procuring Hacking Team's spyware product[63] on behalf of customers in the Viet Nam MOPS (see Figure 20).[64]



Dear Mr Marco Bettini,

Thank you for your prompt answer by email and for your information.

Our main target is Ministry of Public Security of Vietnam , in your particular field , they have several projects in the process. Customer will also be attending tomorrow some exhibition on the

If you are already in touch with end users in Vietnam I do understand and do not want to trouble you overlapping on the same customers. If you can disclose the name of your partner, I car

If it is possible to cooperate on some projects, I have no issue to sign any NDA,

Best Regards

Alexis Delevaux

Figure 20: Leaked email about the purchase of Hacking Team spyware tools on behalf of the Viet Nam Ministry of Public Security in 2011.

Export records[65] obtained by Amnesty International and EIC reveal that on 1 November 2021, 30 items of computer hardware, worth 8.5 million US dollars, were shipped by plane from Delsons Hong Kong Ltd. to Vietnam. The recipient of the goods was "BCA - Thang Long Co., Ltd", a state-owned company established in Viet Nam in 1993 by decree of the Minister of Public Security. One of its activities is import and export for the MOPS as described on its website. [66]

This shipment included a "PC monitoring module", a "control center" and a "mobile smartphone monitoring module" related to a "professional software system" (see Figure 21). These three items, worth 8.4 million dollars, were manufactured by "AS". EIC media partners who reviewed Amnesty International's findings,

[62] Integrated Companies Registry, https://www.icris.cr.gov.hk/csci/ (accessed on 2 October 2023).
[63] Hacking Team was an Italian spyware manufacturer. They produced the Galileo spyware which was sold to numerous countries around the world.
[64] WikiLeaks, "Hacking Team: [BULK] RE: demand information Vietnam following Milipol", 8 July 2015, https://wikileaks.org/hackingteam/emails/emailid/571541
[65] Export records, also known as shipping records or a bill of lading (BOL) is a document by a carrier to acknowledge receipt of the cargo. It lists transport method, declared value, amount of units, shipper, consignee, type of goods, description of goods among others.
[66] BCA – Thang Long Co., Ltd, https://bca-thanglong.vn/ (accessed on 26 September 2023).

confirmed to the organization that "AS" is used as an abbreviation for Advanced Middle East Systems in internal Nexa group documentation. The 27 other items included in the shipment, whose total value was 167,600 US dollars, included Dell servers and desktops, network equipment and a laptop.

Amnesty and EIC obtained information regarding this shipment from three different export records databases. The data is exactly the same regarding all aspects of the shipment (prices, quantity and description of goods, date of delivery, names of companies exporting and importing), except the country of origin. Two of the databases indicate that the goods were shipped from the UAE, whereas the third one indicates that they were shipped from Israel. Contacted by EIC for clarification, Israeli Customs refused to answer regarding this shipment and the government of the UAE government did not respond.

Amnesty International believes that this shipment from Delsons Hong Kong Ltd. is tied to the sale of the Predator spyware system to Viet Nam. Amnesty International sent a letter to Delsons requesting a response on this evidence but has not received a reply at the time of publication. Delsons Hong Kong Ltd. was also approached for a response by EIC.

< 10/13 >

Transaction date	2021/11/01
B/L No.	--
Buyers	Bca Thang Long One Member Limited Company
Supplier	Delsons Hong Kong Ltd.
Import area	Vietnam
Export area	Israel
Product description	MOBILE SMART PHONE MONITORING MODULE BELONGING TO PROFESSIONAL SOFTWARE SYSTEM, MANUFACTURER: AS @ Translate
HS code	84714190
Quantity	1.0 OTHER
Weight	--
Total price	2800000.0
Unit price	2800000.0
POL	--
POD	--
Shipping methods	Air Transport
Contact person	--

Figure 21: Transfer of "mobile smartphone monitoring module" to "BCA.- Thang Long Co" with a declared value of 2.8 million dollars.[67]

Additional shipping records obtained by Amnesty International reveal that "Advanced Middle East Systems" directly shipped computer network components during the same time period in October 2021 to a Vietnamese company named "I-Globe". The company's website describes its business focus as "security, encryption, IT & specialized solutions, dedicated to special government organizations, enterprises...".[68] On its Facebook account "I-Globe" claims to work with the Viet Nam MOPS.[69]

[67] 52wmb.com, Export records, https://www.52wmb.com/ (accessed on 26 September 2023).
[68] I-Globe, https://iglobe.com.vn/en/ (accessed on 26 September 2023).
[69] "i-Globe Techno J. Is Specialised company who serves for customers from MoD, MoPS and other.". See: Facebook, I-Globe Technology Investment & Development Joint Stock Company, 15 November 2021, https://www.facebook.com/connectingworldtechnologies/posts/pfbid025VoHTQp81AUVAskXRK14hRUkZvu48cgnZTCAx5ZnvMBqhW76B8MfsambnDuaU67SI

Figure 22: Screenshot from the i-Globe website

Based on the EIC analysis of internal documents available to the consortium, and the additional shipment information outlined above, Amnesty International believes that Intellexa's Predator spyware was sold from the Nexa group and their "Advanced Middle East Systems" sales branch to a Vietnamese customer in the Viet Nam Ministry of Public Security though a number of international and local broker companies. In a reply letter sent to EIC, representatives of the Nexa group stated that:

> "Advanced Middle East Systems then worked briefly with Intellexa to help commercialize its solutions. Advanced Middle East Systems acted as a reseller/intermediary and was not responsible for export control. It was up to the solution manufacturer to request export authorizations depending on the countries in which the solution was able to be installed.
>
> "On this subject, your information is inaccurate. While it is true that some intermediation contracts were signed, in full compliance with export rules, concerning technologies that you describe as "offensive", none of our contracts were fulfilled. In 2021, we terminated them all before they became operational, because we deemed these technologies to be too controversial."

In an additional response the Nexa representatives confirm that there were contracts established with Viet Nam for offensive cyber technology. However, the representatives claim that the stopped their participation in the spyware component of the contracts and only continued a part of the contract related to cybersecurity:

> "We confirm that the termination of "la lutte informatique offensive (LIO)" ('offensive cyber' products) contracts are authentic and in effect for the countries cited. On Viet Nam, we only kept the part [of the contract] related to cybersecurity. Once again, we have taken the decision to move on and stop all actions in the field of LIO."

EIC followed up to this response from Nexa Technologies to ask about the sales to Viet Nam via Delsons outlined in this section. At the time of publication of this report, no further reply had been received by EIC.

4.6 ATTRIBUTION OF RESPONSIBILITY FOR THE ATTACKS

This case study demonstrates the risk that Intellexa's products pose to the work of human rights defenders, journalists, officials of international institutions and others. This chapter has outlined Amnesty International's Security Lab research into how the operator of the @Joseph_Gordon16 account attempted to infect targets with a 1-click spyware platform. Amnesty International has a high degree of confidence that the attempted attacks described in this report are linked to Intellexa's Predator spyware and associated spyware infrastructure.

The valid and time-limited Predator infection URLs used in this attack could only be generated with access to the backend Predator administrative interface of a customer. This suggest the operator behind the @Joseph_Gordon16 is either a direct customer of Intellexa or an entity with an ongoing and real-time operational relationship with the Intellexa Predator customer. As outlined in the previous section, shipment records and other documentation show that Viet Nam has purchases spyware from the Intellexa alliance.

This newly identified campaign targeted Vietnamese civil society and journalists, as well as political officials working on issues of interest to the government of Viet Nam. The spyware campaign used URLs designed to imitate legitimate Vietnamese websites. Amnesty International shared technical indicators about this attack campaign with researchers at Google's Threat Analysis Group who confirmed to EIC partners that they believe this campaign is "associated with a government actor in Vietnam." Security researchers at Meta have

also previously identified a Cytrox (part of the Intellexa alliance) Predator customer which they believe was based in Viet Nam.[70]

This chapter has also outlined Intellexa's history of selling spyware to Viet Nam, including through drawing on research by EIC partners as part of the "Predator Files" investigation. The combination of technical research and evidence of Intellexa alliance sales to Viet Nam, suggests that the operator of the account had close links to Viet Nam and may have been acting on behalf of Vietnamese authorities or interest groups. Amnesty International shared these findings with the Vietnamese authorities prior to publication. At the time of publication of this report, we have not received any response.

[70] Meta, *Threat Report on the Surveillance-for-Hire Industry* (previously cited), https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

5. HUMAN RIGHTS IMPLICATIONS RELATED TO THE USE OF SPYWARE

5.1 BAN ON HIGHLY INVASIVE SPYWARE

Targeted digital surveillance can be lawfully conducted by states only in the presence of adequate human rights safeguards to prevent abuse. International human rights standards require that targeted surveillance take place only on the basis of individualized reasonable suspicion, in accordance with the law, when is strictly necessary to meet a legitimate aim, and when it is conducted in a manner that is proportionate to that aim and non-discriminatory.[71]

However, even a human rights compliant regulatory framework would be inadequate to prevent human rights violations linked to the use of certain types of highly invasive spyware. Highly invasive spyware allows unlimited access to a device and its use cannot be independently audited. Such highly invasive spyware can never be used in a human rights compliant manner and should be permanently banned. As noted by the European Data Protection Supervisor, with the use of such highly invasive tools, "The level of interference with the right to privacy is so severe that the individual is in fact deprived of it. In other words, the essence of the right is affected. Therefore, its use cannot be considered proportionate – irrespective of whether the measure can be deemed necessary."[72] This aligns with the reasoning presented by the UN Special Rapporteur on Counterterrorism, who argues that spyware that it is incapable of being meaningfully limited in its functionality, and whose use cannot be audited independently, should be subject to a ban.[73]

Predator spyware, and its rebranded variants, are highly invasive spyware that can access unlimited amounts of data on the device by default and cannot, at present, be independently audited. Due to this, it cannot be determined whether it can be limited in its functionality presently. As such, Amnesty International's assessment is that Predator is highly invasive spyware, and therefore no deployment of Predator can be human rights compliant.

Similarly, strategic infection systems resemble mass surveillance tools as they require access to large-scale internet traffic to target and infect individuals.[74] Amnesty International considers that there cannot exist a reasonable justification to conduct indiscriminate mass surveillance. All indiscriminate mass surveillance fails to meet the test of necessity and proportionality, which requires states to use the least rights restrictive

[71] International Convenant on Civil and Political Rights, *General comment No. 34*, 12 September 2011, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf
[72] European Data Protection Supervisor, *Preliminary Remarks on Modern Spyware*, 15 February 2022, p. 8.
[73] UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*, April 2023, https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf, para. 66.
[74] Amnesty International, "Predator Files: Technical deep-dive into Intellexa Alliance surveillance products" (previously cited), https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/

tool available for surveillance. Mass surveillance cannot meet these tests as it gathers unlimited amounts of data, and its use cannot be human rights compliant.

5.2 FAILURE OF EXISTING HUMAN RIGHTS SAFEGUARDS

The use of highly invasive spyware such as Predator should be globally banned due to the risks it poses to human rights. Other types of less invasive spyware that can be limited in functionality and whose use can be independently verified and audited should be subject to a moratorium, pending the development of human rights safeguards capable of preventing its abuse. Such safeguards would include, for example, regulating the export of surveillance technologies such that it ensures the denial of export authorizations where there is a substantial risk that the export in question could be used to violate human rights, implementing domestic legislation that imposes safeguards against human rights violations and abuses through digital surveillance, and establishing accountability mechanisms designed to provide victims of surveillance abuses a pathway to remedy, among others.

Amnesty International and numerous other civil society organizations,[75] alongside the Office of the High Commissioner for Human Rights,[76] several UN and regional-level experts,[77] and at least one state, Costa Rica,[78] have called for a moratorium on the sale, transfer, export, and use of all spyware until such a time as an adequate system of human rights safeguards are in place.

In the aftermath of the Pegasus Project disclosures, there has been some progress on the regulation of spyware. The U.S. Government's Bureau of Industry and Security has put multiple spyware companies on its entity list for malicious cyber activities, including two corporate entities of the Intellexa surveillance alliance, as well as notorious spyware vendors like the NSO Group and Candiru.[79] The White House issued an Executive Order prohibiting the U.S. government from using commercial spyware that "poses significant counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government or foreign person".[80] In addition, eleven states have come together to announce efforts to counter the proliferation and misuse of commercial spyware.[81] At the Summit for Democracy, 45 states endorsed new guiding principles on the government use of surveillance technologies.[82] Led by the United States, some states have signed on to an Export Controls and Human Rights Initiative Code of Conduct.[83] Litigation and various country-level investigations are open in multiple jurisdictions, such as in Thailand, the USA, the UK, Israel, Spain, France, Hungary, Poland, and India, among others.[84] Earlier this year, the

---

[75] Amnesty International, *Global Digital Compact: joint submission on targeted surveillance* (Index: IOR 10/6726/2023) 1 May 2023, https://www.amnesty.org/en/documents/ior10/6726/2023/en/

[76] UN Office of the High Commissioner for Human Rights (OHCHR), Report: *The right to privacy in the digital age*, August 2022, A/HRC/51/17.

[77] United Nations, "Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech", 12 August 2021, https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening; Organización de los Estados Americanos, "CIDH y RELE: República Dominicana debe investigar espionaje a través de Pegasus a periodista de investigación", 1 June 2023, https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2023/106.asp; UN Human Rights Council, Report of the Working Group on Enforced or Involuntary Disappearances, 11 September 2023, A/HRC/54/22/Add.5, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G23/182/83/PDF/G2318283.pdf?OpenElement, para. 21.

[78] Access Now, "Stop Pegasus: Costa Rica is the first country to call for a moratorium on spyware technology", 13 April 2022 (updated on 26 January 2023), https://www.accessnow.org/press-release/costa-rica-first-country-moratorium-spyware/

[79] U.S. Department of State, "The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities", 3 November 2021, https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities/; U.S. Department of State, "The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities" (previously cited),https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities-2/

[80] White House, "Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security", 27 March 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/

[81] White House, "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware", 30 March 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/

[82] U.S. Department of State, "Guiding Principles on Government Use of Surveillance Technologies", 30 March 2023, https://www.state.gov/guiding-principles-on-government-use-of-surveillance-technologies/

[83] U.S. Department of State, "Export Controls and Human Rights Initiative Code of Conduct Released at the Summit for Democracy", 30 March 2023, https://www.state.gov/export-controls-and-human-rights-initiative-code-of-conduct-released-at-the-summit-for-democracy/#:~:text=The%20Export%20Controls%20and%20Human,technology%20that%20violate%20human%20rights

[84] Citizen Lab, "Litigation and other formal complaints related to mercenary spyware", 12 December 2018 (updated on 31 July 2023), https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/#NSO

European Parliament concluded the PEGA Committee of Inquiry to investigate the use of Pegasus and equivalent spyware, condemning spyware abuses in several EU member states and calling for reform.

These are significant and welcome steps in the right direction. However, public declarations, recommendations, and voluntary commitments have not always translated into decisive action, and those unlawfully targeted with spyware around the world have not yet received meaningful accountability or remedies. While some states have initiated certain voluntary efforts as noted above, others have stone-walled investigations and failed to provide meaningful transparency. For example, prosecutors in Hungary terminated their probe into unlawful use of Pegasus in the country, citing "no unauthorized and secretive collection of information or use of a concealed device".[85] In Spain, a Barcelona court had to suspend an investigation due to lack of progress on rogatory information from Israeli authorities.[86] In 2021, the Supreme Court of India set up a technical committee to investigate abuses involving the use of Pegasus. In 2022, the committee concluded their investigation, but the court has not made the findings of the report public.[87] The court further noted that the Indian authorities "did not cooperate" with the technical committee's investigations.[88]

The devastating consequences of unlawful and unchecked surveillance continue, violating the right to privacy, freedom of expression, association, and peaceful assembly of those targeted. The impact on women human rights defenders,[89] and the use of spyware against those facing multiple and intersecting forms of discrimination on the ground of race, ethnicity, religious identity, disability, and sexual orientation and gender identity, continues to be particularly devastating. Racialized women, women from ethnic or religious minorities, lesbian, bisexual, transgender women as well as gender diverse individuals, and women with disabilities are exposed to unique and compounded harms.

In addition, when spyware continues to operate unchecked without any safeguards, it has a chilling effect on human rights work, where activists self-censor out of fear of surveillance.[90] Furthermore, the impact goes beyond those individuals who are targeted. It affects anyone who may refrain from exercising their rights to free expression, association and peaceful assembly, amongst others, due to the ways in which data regarding their activities could be used against them.

These latest disclosures show that civil society, including media outlets, journalists, and academic researchers continue to face the scourge of unregulated spyware. In addition, the targeting of regional, national, and international official authorities, including diplomatic targets, shows once again what Amnesty International has long been warning about. Commercial spyware has severe implications both for human rights and the security of the digital ecosystem as a whole. Unregulated, these cyber weapons can and have been turned back on third governments and authorities.

Recent voluntary efforts by states add to existing initiatives like the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods, where participating states agree to harmonize export regimes. However, the Wassenaar Arrangement is not legally binding, and relies on voluntary undertakings by states. Amnesty International has previously noted the Arrangement's mandate does not include the protection of human rights.[91] Indeed, noting the non-binding nature of it, in its recommendations to the European Council and European Commission following the PEGA committee investigation, the European Parliament called for the Wassenaar Arrangement to become a binding agreement, and stressed that it should include a human rights framework as part of its assessment of export licenses.[92]

The implementation of these voluntary declarations by states needs to be closely monitored to see if states are indeed abiding by their public commitments and doing what they promised. There need to be more concerted efforts by states to put in place binding and enforceable human rights safeguards at a national, regional and international level.

---

[85] Al Jazeera, "Hungary prosecutors open investigation into Pegasus spying claims", 22 July 2021, https://www.aljazeera.com/news/2021/7/22/hungary-prosecutors-open-investigation-into-pegasus-spying-claims
[86] El Nacional, "Judge suspends first Catalan espionage case; lawyer demands reopening and widening", 30 May 2022, https://www.elnacional.cat/en/politics/judge-closes-torrent-maragall-pegasus-spyware-catalonia_765453_102.html
[87] The Guardian, "Indian supreme court orders inquiry into state's use of Pegasus spyware", 27 October 2021 https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware
[88] The Wire, "Pegasus: Malware Found in 5 Phones, Government 'Refused to Cooperate' With Probe, Says CJI", 25 August 2022, https://thewire.in/law/supreme-court-pegasus-technical-committee
[89] Access Now, "Unsafe anywhere: women human rights defenders speak out about Pegasus attacks", 17 January 2022 (updated on 8 May 2023), https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/
[90] OHCHR, Report: *The Right to Privacy in the Digital Age*, 30 June 2014, UN Doc. A/HRC/27/37, para. 20.
[91] Amnesty International, *Operating from the Shadows: Inside NSO Group's Corporate Structure* (previously cited), https://www.amnesty.org/en/documents/doc10/4182/2021/en/
[92] European Parliament, *Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation)*, 15 June 2023, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.pdf, Recommendations 54 and 56.

In 2019, the former UN Special Rapporteur on Freedom of Opinion and Expression noted "It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists."[93] Amnesty International believes that despite initial progress, this continues to be the case. Companies and their state clients continue to operate in secrecy to unleash invasive spyware on civil society and journalists for no other reason than exercising their human rights and doing work to protect the rights of others. The latest disclosures should serve as a reminder that more meaningful and concerted state action at national and international level is necessary.

5.3 HUMAN RIGHTS OBLIGATIONS OF STATES

Nation states have binding obligations under international human rights law to protect human rights from abuse by third parties.[94] This includes the obligation to regulate the conduct of companies who are domiciled there or are under their effective control in order to prevent them from causing or contributing to human rights abuses even if they occur in other countries.[95]

However, the Predator Files disclosures confirm what we have long known – that many states have little interest in respecting, let alone protecting human rights, when it comes to surveillance. The failure of states where the Intellexa alliance's corporate entities are based– for example, Greece, Ireland, France, Germany, the Czech Republic, Cyprus, Hungary, Switzerland, Israel, North Macedonia, and the UAE – to put a meaningful check on the Intellexa alliance has led to human rights abuses.[96]

5.4 CORPORATE RESPONSIBILITY TO RESPECT HUMAN RIGHTS

As laid out in the UN Guiding Principles, companies also have a responsibility to respect human rights wherever they operate in the world. The UN Guiding Principles outline that companies should take proactive steps to ensure that they do not cause or contribute to human rights abuses across all their operations, and to respond to any human rights abuses if and when they do occur. In order to meet that responsibility, companies must carry out human rights due diligence to "identify, prevent, mitigate and account for how they address their human rights impacts." The corporate responsibility to respect human rights exists beyond its own operations. It also exists independently of a state's ability or willingness to fulfil its own human rights obligations and over and above compliance with national laws and regulations protecting human rights.[97]

This also includes the company's responsibilities to account for adverse human rights impacts in its full value chain, including the use of its products and services. The UN Guiding Principles note that, "Business enterprises may be involved with adverse human rights impacts either through their own activities or as a result of their business relationships with other parties... 'business relationships' are understood to include relationships with business partners, entities in its value chain, and any other non-State or State entity directly linked to its business operations, products or services."[98] Within this context, a company that sells

---

[93] UN Human Rights Council, *Report of the Special Rapporteur on freedom of opinion and expression*, 28 May 2019, UN Doc. A/HCR/41/35, https://undocs.org/A/HRC/41/35, para. 46.
[94] UN Human Rights Committee (HRC), General Comment 31 [80]: *The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, 26 May 2004, UN Doc. CCPR/C/21/Rev.1/Add. 13, para. 8.
[95] States are responsible for protecting against abuses by private companies even outside of their borders. This principle is well-accepted and directly applicable to rights infringed in the cases revealed in this project. See, for example, UN Committee on Economic, Social and Cultural Rights (CESCR), General Comment 14: *State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities*, 10 August 2017, UN Doc. E/C.12/GC/24, § III.C.2.; UN Human Rights Committee (HRC), General Comment 36: *Right to Life*, 3 September 2019, UN Doc. CCPR/C/GC/36, para. 63; UN Special Rapporteur on extrajudicial, summary or arbitrary executions, Annex to the Report: *Investigation into the unlawful death of Mr. Jamal Khashoggi*, 19 June 2019, UN Doc. A/HRC/41/CRP.1.
[96] Limited progress was made in January 2023, the Hellenic Data Protection Authority (HDPA) reportedly fined Intellexa A.E. €50,000 for violation of the General Data Protection Regulation (Regulation (EU) 2016/679) on the ground that the company had failed to provide all the information. See: Haaretz, "Greek Authorities Fine Spyware Firm Owned by Former Israeli Intel Officer", 16 January 2023, https://www.haaretz.com/israel-news/security-aviation/2023-01-16/ty-article/.premium/greek-authorities-fine-intellexa-chief-over-spyware-scandal/00000185-bab3-deab-ad97-fafbd8ae0000
[97] OHCHR, *Guiding Principles on Business and Human Rights*, 2011, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
[98] OHCHR, *Guiding Principles on Business and Human Rights* (previously cited), https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf, Guiding Principle 13

surveillance equipment could be complicit in any subsequent violation of human rights in which the equipment it supplies is used. An International Commission of Jurists (ICJ) Panel of Experts has examined the question of corporate complicity in human rights violations in some depth and clarified how legal liability, both civil and criminal, could arise for such complicity. The ICJ panel considered that there could be a sufficiently close link in law if the company's conduct enabled, exacerbated or facilitated the abuse, and the company knew, or ought reasonably to have known, that the abuse would occur. A company could enable, exacerbate or facilitate abuse through, among other things, the provision of goods or services.[99]

The companies in the Intellexa alliance have themselves not proactively disclosed any information about their human rights due diligence practices. Any assessments, if they exist, about the human rights impacts of their surveillance technologies remain shrouded in secrecy. Amnesty International wrote to the Intellexa alliance with a request for comment on the information detailed in this report and asked them to share information about their human rights due diligence practices, including whether they had conducted detailed human rights due diligence in each of the end-user countries to whom they sell their products. At the time of publication of this report, Amnesty International did not receive a response.[100]

[99] International Commission of Jurists (ICJ), *Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes*, 1 January 2008, icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-international-crimes

[100] EIC did receive a response from former Nexa group executives and main shareholders on behalf of their companies including Nexa Technologies and Advanced Middle East Systems. Their responses to EIC that were relevant to the questions sent to them by Amnesty International are included in section 4.1, above.

6. "EU BASED AND REGULATED"

6.1 FAILURE OF EUROPEAN UNION AND MEMBER STATES TO END SPYWARE ABUSE

The latest disclosures paint a dismal picture of failures of the European Union and its member states to rein in unaccountable companies and errant member states who continue to take advantage of the conspicuously large cracks in the regulatory systems at the regional and national levels within the EU. The brazen surveillance campaign detailed in this report using the Intellexa alliance's tools shows the very direct risks and impacts of the proliferation of cyber-surveillance tools from EU-based and regulated companies to third-country operators, which have then been used to target individuals and institutions within the European Union, and elsewhere.

The Predator Files disclosures show that export licences for surveillance technologies were granted to corporate entities within the Intellexa alliance in France.[101] In addition, the European Parliament investigation into the use of Pegasus and other Equivalent Spyware (PEGA) committee report notes that Greek authorities have granted export licenses to Intellexa for the sale of Predator to Madagascar and Sudan.[102]It is not clear if these member states conducted any assessment of the risks they represent to the violation of human rights before approving these export licences. Whether export licences were sought and granted by other EU member states is also unclear, as are the details of any relevant human rights assessments conducted as part of the licensing process.

The "Predator Files" disclosures further show that export control mechanisms in the EU member states, particularly in France, have been circumvented, where exports have reportedly occurred without the authorisation of the French authorities. Exports have instead, reportedly happened from an Intellexa alliance entity in the UAE, thus evading EU regulation.[103]

Exports of spyware from the EU are subject to licensing under the Dual-Use Export Regulation, which should in theory take account of human rights risks posed by such exports. Given that export licences were granted where there is a substantial risk of human rights violations by the end users, as well as the circumvention of EU export control regulations aided through opaque corporate structures and entities in third countries, it is clear that the EU Dual-Use Export Regulation has significant shortcomings, which have serious implications for human rights both within and outside the EU. For example, in its annual report, the European Commission does not provide any information on what type of products have been exported to what

[101] EIC, Projects, https://eic.network/#projects
[102] European Parliament, *Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation)* (previously cited), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.pdf, para Q.
[103] EIC, Projects, https://eic.network/#projects

countries and who has provided the licence[104] and therefore fails to meet the transparency requirements necessary for a human rights accountability landscape.[105] Two years after the publication of the Recast Dual Use Regulation there is still no guidance from the Commission on how to conduct human rights risks assessments related to the export of cyber surveillance technologies to assist states and licensing authorities.[106]

While the methods of targeting outlined in this report here have been haphazard, the potential harms resulting from the wide proliferation of cyber-surveillance tools to states with dismal human right records and/or who lack adequate human rights safeguards in law are very clear: not only do they lead to human rights violations abroad but they are also a threat to security and human rights within the EU, having been found to have been used to target EU officials themselves.

6.1.1 EU REGULATORY ACTION

In the aftermath of the Pegasus Project disclosures, the European Parliament launched an investigation into the use of Pegasus and other Equivalent Spyware (PEGA). After a year of hearings and investigations, the PEGA Committee adopted recommendations to the EU Council and Commission which noted that significant breaches of EU law had taken place and called for meaningful action from the EU and its member states through detailed, but non-binding, recommendations.

The European Parliament's PEGA committee also pointed to the lack of political will of the European Union and its member states by noting that, "most member state governments and member state parliaments have not provided the European Parliament with meaningful information about their legal frameworks governing the use of spyware beyond what was already publicly known,"[107] and more damningly, "concludes that neither the Member States, nor the Council, nor the Commission seemed to be at all interested in maximising their efforts to fully investigate the spyware abuse, thus knowingly protecting Union governments which violate human rights within and outside of the Union".[108]

As noted above, voluntary mechanisms like the Wassenaar Arrangement and the recent move by some EU member states to join the Summit for Democracy[109] efforts led by the United States to counter spyware misuse are welcome but remain non-binding commitments. Investigations launched in multiple member states – Hungary, Spain, and Greece – after the Pegasus Project and previous Predator-related revelations in Greece have not yet led to accountability and remedy for the victims of the spyware.[110]

Regulatory efforts in the EU are thus severely inadequate or lacking proper enforcement. For years, civil society has warned that the EU dual-use export control rules – designed to prevent human rights abuses through licensing of EU spyware exports (see above 6.1) – are not fit for purpose to prevent against the human rights consequences of exporting to countries where there is a significant risk of human rights violations. Despite civil society warnings, the recast dual-use export regulation adopted in 2021 requires only that states "consider", rather than require, human rights criteria as part of their assessment when granting export licenses but leaves them free to grant them all the same.[111] Such loopholes in the regulation give states free rein to ignore the human rights risks related to the export of these tools. Civil society has long been calling for human rights safeguards, including greater transparency in the reporting of exports, which

---

[104] European Commission, *Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items,* 1 September 2022, https://ec.europa.eu/transparency/documents-register/api/files/COM(2022)434_0/090166e5f0bc60c8?rendition=false

[105] Access Now, *Human Rights Organizations' Response to the Adoption of the New EU Dual Use Export Control Rules,* March 2021, https://www.accessnow.org/wp-content/uploads/2021/03/Analysis-EU-Surveillance-Tech-Export-Rules.pdf
CIRCABC, 14 June 2023, https://circabc.europa.eu/ui/group/654251c7-f897-4098-afc3-6eb39477797e/library/e7dc5aae-bce0-4f45-b1e5-bb15b272b66b?p=1&n=10&sort=modified_DESC

[107] European Parliament, *Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation)* (previously cited), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.pdf, para. V.

[108] European Parliament, *Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation)* (previously cited), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.pdf, Article 13.

[109] U.S. Department of State, "Guiding Principles on Government Use of Surveillance Technologies" (previously cited), https://www.state.gov/guiding-principles-on-government-use-of-surveillance-technologies/

[110] In December 2022, the Greek parliament passed a controversial bill that lacked effective safeguards for individuals subjected to surveillance and legalized the use of spyware technology by the authorities. See: Amnesty International, "Greece's surveillance scandal must shake us out of complacency", 26 January 2023, https://www.amnesty.org/en/latest/news/2023/01/greeces-surveillance-scandal-must-shake-us-out-of-complacency/

[111] European Parliament and the Council of the European Union, *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items* (recast), 11 June 2021, PE/54/2020/REV/2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0821

should be broken down and published annually by end user, destination, and intended use, the government agency involved, the value of the license, and whether the license was granted or denied and why.[112]

6.2 MANDATORY CORPORATE HUMAN RIGHTS DUE DILIGENCE

The PEGA Committee has called for additional European legislation that requires corporate actors producing and/or exporting surveillance technologies to include human rights due diligence frameworks, in line with the UN Guiding Principles.[113] The European Union is currently negotiating the Corporate Sustainability Due Diligence Directive (CSDDD) which, if enacted, will require companies of a certain size from all sectors operating in the EU to conduct human rights and environmental due diligence to assess and address the human rights risks and impacts of their operations and value chain.

The CSDDD provides a timely opportunity to begin to address the harms of the surveillance industry. However, loopholes in the proposals put forward by the EU co-legislators could mean the CSDDD is not properly applied to surveillance technology companies. For example, the Directive is likely to apply to only very large companies which may exclude certain companies from the scope of the law, including companies in the Intellexa alliance.

Furthermore, the European Parliament and EU Council have proposed that companies should not have to assess how their products and services may be misused as part of their human rights and environmental due diligence under the Directive.[114] There has also been an attempt by the EU Council to introduce an exemption for companies that produce products subject to export control which would include surveillance technologies.

[112] Access Now, *Human Rights Organizations' Response to the Adoption of the New EU Dual Use Export Control Rules*, March 2021, https://www.accessnow.org/wp-content/uploads/2021/03/Analysis-EU-Surveillance-Tech-Export-Rules.pdf
[113] European Parliament, *Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation)* (previously cited), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.pdf, Recommendation 66.
[114] To read more about Amnesty International's analysis of the CSDDD proposals, see Amnesty International, *Closing the loopholes: Recommendations for an EU corporate sustainability law which works for rights holders* (Index: IOR 60/6539/2023), 15 May 2023, https://www.amnesty.org/en/wp-content/uploads/2023/05/IOR6065392023ENGLISH.pdf

7. RECOMMENDATIONS

TO THE EUROPEAN UNION AND ITS MEMBER STATES:

Recommendations for action within the European Union

- All EU member states that have granted export licences to the Intellexa alliance should immediately revoke the licences, and conduct an independent, impartial, transparent investigation to determine the extent of possible unlawful targeting, to culminate in a public statement on the results of these efforts and steps to prevent future harm.
- EU member states should impose a ban on highly invasive spyware, whose functionality cannot be limited to only those functions that are necessary and proportionate to a specific use and target, or whose use cannot be independently audited.
- EU member states must implement a human rights regulatory framework that governs surveillance and that is in line with international human rights standards. Until such a framework is implemented, a moratorium on the purchase, sale, transfer, and use of all other spyware should be enforced.
- EU member states must ensure effective remedy to victims of unlawful targeted surveillance and hold perpetrators to account for the violations. Further, member states must commit to reforming existing laws that pose barriers to remedy for these victims and ensure that both judicial and nonjudicial paths to remedy are available in practice.
- EU member states must adopt and enforce legislation that requires all corporate actors to respect human rights and implement human rights due diligence measures in line with the UN Guiding Principles. Corporate actors should be required to identify, prevent, and mitigate all potential and actual adverse human rights impacts of their operations and throughout their value chain. Therefore, as part of the ongoing deliberations on the Corporate Sustainability Due Diligence Directive (CSDDD), the EU should:
    - Require companies to conduct human rights due diligence with respect to the full value chain including the purchase, sale, transfer, export and use of products.
    - Require companies operating in all sectors to implement the requirements on the CSDDD including those producing spyware, as well as financial institutions
- EU member states must adopt and implement domestic legislation that imposes safeguards against human rights violations and abuses resulting from unlawful digital surveillance. This should be in line with the 2015 European Court of Human Rights judgment in ***Roman Zakharov v. Russia***, as well as the Necessary and Proportionate Principles.
- EU member states and the European Commission should ensure the robust implementation of the EU Export Control Rules that entered into force on 9 September 2021 with the recast Dual Use Regulation. This includes taking immediate action toward underscoring the human rights due diligence obligations that follow from the Dual-Use Regulation and creating a transparent market in cybersurveillance technologies that is bound by effective human rights safeguards.
    - The Regulation establishes that the Commission shall publish an annual public report to the Parliament and Council. These reports should at a minimum include the number of license applications per item, the exporter name, a description of the end user, destination, and intended use, the government agency involved, the value of the license, and whether the license was granted or denied and why.

- Further, transaction screening measures by member states should include an assessment of the strategic nature of the items and the risks they represent to the violation of human rights. National authorities should report on the implementation of due diligence responsibilities and obligations and encourage companies to inform the public about the scope, nature, and findings of the human rights due diligence procedures they implemented.
- Member states should ensure that exporting countries establish mechanisms to provide effective remedy for human rights violations committed using the transferred technology. The guidelines that will be published pursuant to art. 26(1) Dual-Use Regulation 2021/821/EU, must detail requirements for internal compliance programs and due diligence that is expected from exporters in the Dual-Use Regulation based on the United Nations Guiding Principles on Business and Human Rights (UN Guiding Principles) and the OECD Guidelines for Multinational Enterprises.
- The European Commission should immediately conduct an investigation into all EU and member states' export licenses granted, including EU General Export Authorisation EU005 that includes software designed for the use of monitoring and interception equipment, and ensure that EU members states revoke all marketing and export licenses in situations where there is a significant risk that such technology could contribute to human rights violations. If member states' granting of export licenses are found to be in violation of export regulation standards, the European Commission should initiate infringement proceedings.

- EU member states should take robust action on ending transnational repression of human rights defenders (HRDs) and journalists within the EU by ensuring that any EU internal instrument on HRDs includes commitments to counter transnational repression of HRDs, including unlawful targeted surveillance.

Recommendations for action by the European Union and its member states through their foreign policy instruments

Given its ambition to be a global standard setter on human rights, the EU and its member states can and must play a role in ensuring the protection of human rights and adherence to the rule of law in the digital realm at home and abroad. This is rooted in the EU's and its member states' human rights obligations to protect and promote human rights globally as laid out in the Article 21 of The Lisbon Treaty. Further, this aligns with EU commitments in the Council Conclusions on Shaping Europe's Digital Future, the EU action plan on Human Rights and Democracy and the EU's human rights guidelines. EU leaders, including Commission President Von Der Leyen and High Representative Borrell, have already underlined the importance of protecting civil society and upholding the right to privacy and freedom of expression online in the digital age.

- The EU and its member states must clearly articulate their position on unlawful targeted surveillance, including through official statements:
  - Express concern about the targeting of journalists, activists and political figures, stressing that such practices are unacceptable and violate the rights to freedom of expression, peaceful assembly and privacy.
  - Stress the urgent need for greater transparency and legal accountability of the surveillance industry in light of the rising digital attacks and targeted surveillance of human rights defenders, journalists and civil society by governments seeking to silence and intimidate such actors around the world.
  - Call on states to take urgent measures toward ensuring greater regulation over the cybersurveillance industry, accountability for related human rights violations and greater oversight over this poorly-regulated industry.
- The EU and its member states should reach out bilaterally to organize démarches toward the relevant authorities in Viet Nam.
- The EU and its member states should seek clarifications from the Vietnamese authorities and, among other things:
  - Urge the relevant authorities to conduct an immediate, independent, transparent and impartial investigation of any cases of unlawful surveillance, and where appropriate, pursue legal avenues to provide remedies to victims and hold perpetrators to account, in accordance with international human rights standards.

- Underline that the use of spyware for surveillance is lawful only when it meets certain strict criteria, as set out in international human rights law, and that any such surveillance must be lawful, necessary, proportionate, and time bound.
- Urge authorities in Viet Nam to uphold their obligations and commitments under international human rights law, including those outlined in the ICCPR and the UN Declaration on human rights defenders.
- Raise the cases of targeted human rights defenders, journalists and activists in Viet Nam and in EU member states with the authorities at the highest levels and offer these individuals political, technical and other support in line with the EU guidelines on human rights defenders, the EU guidelines on freedom of expression and the EU action plan on human rights and democracy.
- Urge the Viet Nam government to end all unlawful targeted surveillance of Vietnamese human rights defenders and activists abroad, including in EU member states, and make it clear that such transnational repression is unacceptable.

- EU member states must call on exporting states in third countries to immediately revoke all marketing and export licences issued to Intellexa and conduct an independent, impartial, transparent investigation to determine the extent of unlawful digital surveillance using Intellexa's tools. This should include a full review and subsequent reform of the export licensing regime to ensure that it is fit for purpose in law and practice, and it prevents future human rights abuses related to the export of cybersurveillance equipment from their jurisdictions. This should culminate in public disclosure of results of the investigation and steps taken to prevent future abuses.
- In line with the Council Conclusions of 20 February 2023 on EU priorities in UN human rights fora, the EU and its member states should participate in key multilateral efforts, including at the UN Human Rights Council, UN General Assembly, and Universal Periodic Review cycles, to develop robust human rights standards that govern the development, sale, transfer, and use of surveillance equipment, and identify impermissible targets of digital surveillance. This includes by supporting the call for a ban on the use of highly invasive spyware.

THE GOVERNMENT OF VIET NAM SHOULD:

- Publicly commit to immediately stopping the use of spyware to unlawfully target human rights defenders, civil society, and journalists within and outside Viet Nam.
- Conduct an independent, impartial, and transparent investigation into the unlawful targeted surveillance mentioned in this report, including investigating whether there are links between this spyware campaign and any specific government agencies.
- Implement a human rights regulatory framework that governs surveillance that is in line with international human rights standards. Until such a framework is implemented, a moratorium on the purchase, sale, transfer, and use of all spyware should be enforced.
- Repeal or revise Articles 117, 118 and 331 of the 2015 Criminal Code, which unduly restrict the rights to freedom of expression, peaceful assembly and association, in order to bring them into conformity with international human rights law.
- Undertake a review and amendment of the Law on Cybersecurity to bring it into conformity with international human rights law, and in particular:
- Repeal or amend Articles 8, 16, 17 and 26 of the Law on Cybersecurity so that they align with international human rights standards governing freedom of expression;
  - Include specific safeguards against arbitrary and discriminatory application of the law;
  - Remove all provisions that would compel internet or tech companies to disclose personal data without adequate safeguards to prevent abuse.
- Repeal or amend Articles 99, 100 and 101 of Decree 15/2020/ND-CP so they align with international human rights standards governing freedom of expression and the right to privacy.
- Repeal or amend Articles 5, 22 and 25 of Decree 72/2013/ND-CP so they align with international human rights standards governing freedom of expression and the right to privacy, and refrain from introducing the currently proposed amendment to the Decree, in particular the proposed amendments under Article 23.d.

ALL STATES SHOULD:

- Enforce a ban on highly invasive spyware, whose functionality cannot be limited to only those functions that are necessary and proportionate to a specific use and target, or whose use cannot be independently audited.
- Implement a human rights regulatory framework that governs surveillance and that is in line with international human rights standards. Until such a framework is implemented, a moratorium on the purchase, sale, transfer, and use of all spyware should be enforced.
- Legally require surveillance companies to conduct human rights due diligence in relation to their global operations including the use of their products and services.
- Adopt and enforce a legal framework requiring transparency by private surveillance companies, including information on self-identification/registration; products and services offered and sales.
- Disclose information about all previous, current and future contracts with private surveillance companies by responding to requests for information or by making proactive disclosures.
- Furthermore, States must, at a minimum, implement the below recommendations if the moratorium on the sale and transfer of spyware equipment is to be lifted:
    - Implement domestic legislation that imposes safeguards against human rights violations and abuses through digital surveillance and establishes accountability mechanisms designed to provide victims of surveillance abuses a pathway to remedy.
    - Reform existing laws that pose barriers to remedy for victims of unlawful surveillance and ensure that both judicial and non-judicial paths to remedy are available in practice.
    - Implement procurement standards restricting government contracts for surveillance technology and services to only those companies which demonstrate that they respect human rights in line with the UN Guiding Principles and have not serviced clients engaging in surveillance abuses.
    - Regulate the export of surveillance technologies, including to:
        - Ensure the denial of export authorizations where there is a substantial risk that the export in question could be used to violate human rights or where the destination country has inadequate legal, procedural and technical safeguards in place to prevent abuse.
        - States should update export control criteria to take account of the human rights record of the end user as well as the legality of the use of sophisticated surveillance tools in the country of destination, stipulating that applications shall be rejected if they pose a substantial risk to human rights.
        - Ensure that all relevant technologies are scrutinized for human rights risks prior to transfer as part of the licensing assessment.
        - Ensure transparency regarding the volume, nature, value, destination and end-user countries of surveillance transfers, for example by publishing annual reports on imports and exports of surveillance technologies.
        - Reform any existing legislation that imposes overly broad restrictions on disclosures of such information.
        - Ensure that encryption tools and legitimate security research are not subject to export controls.
- Participate in key multilateral efforts to develop robust human rights standards that govern the development, sale and transfer of surveillance equipment, and identify impermissible targets of digital surveillance.
- Establish community public oversight boards to oversee and approve the acquisition or use of new surveillance technologies, with powers to approve or reject based on the states' human rights obligations, provisions for public notice and reporting.

THE INTELLEXA ALLIANCE SHOULD, AT A MINIMUM:

- Cease the production and sale of Predator, or other similar highly invasive spyware that does not include technical safeguards allowing its lawful use under a human right respecting regulatory framework.
- Immediately terminate the use, support and sale of its technologies in states where cyber surveillance software has been misused to unlawfully target HRDs, journalists and members of civil society.
- Provide adequate compensation or other forms of effective redress to victims of unlawful surveillance.
- Urgently take proactive steps to ensure that it does not cause or contribute to human rights violations or abuses, and to respond to any human rights abuses when they do occur. In order to meet that responsibility, the Intellexa alliance must carry out human rights due diligence in line with international business and human rights standards, and take steps to ensure that HRDs, journalists and civil society do not continue to become targets of unlawful surveillance using Intellexa alliance technologies.
- Ensure transparency regarding the volume, nature, value, destination, and end user of its surveillance technology transfers.

8. ANNEXES

ANNEX I – INDICATORS OF COMPROMISE

Intellexa Predator domains linked to this campaign

The earliest Predator infrastructure used in this campaign was registered in July 2022. Earlier Predator domains which used Vietnamese themes were first observed in March 2022. New Predator infrastructure associated with the attack domains used in this campaign continued to be active in September 2023.

DOMAIN NAME	FIRST SEEN
ietnamnews[.]com	2022-03-23
lnktonews[.]co	2022-07-19
witteridea[.]co	2022-07-19
caavn[.]org	2022-08-05
xuatnhapcanhvn[.]info	2022-08-05
tokhaiytehanoi[.]org	2022-08-05
southchinapost[.]net	2023-05-02
scanningandinfo[.]online	2023-05-09
asean-news[.]net	2023-05-09
southchinapost[.]co	2023-06-08
asean-news[.]co	2023-06-08
scanningandinfo[.]co	2023-06-08
newsworldsports[.]co	2023-07-13

Table 7: Intellexa Predator domains linked to this campaign.

X (Twitter) accounts linked to this campaign

ACCOUNT	FIRST SEEN	LAST SEEN ACTIVITY
Joseph_Gordon	2019-10-01	Early June 2023
AlexMarcos71	2023-04-04	2023-05-16

Table 8: X (Twitter) accounts linked to this campaign.

Facebook accounts linked to this campaign

ACCOUNT	ACCOUNT NAME	FIRST SEEN	LAST SEEN ACTIVITY
https://www.facebook.com/profile.php?id=100090236330335	Ahn Tran	2023-02-10	2023-03-23

Table 9: Facebook accounts linked to this campaign.

ANNEX II – TWEETS

This annex lists all observed social media posts from the "@Joseph_Gordon16" account which included attack links.

DATE	TO	URL	PLATFORM
12-Apr-23	@CollinSLKoh	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
12-Apr-23	@CollinSLKoh	https://lnktonews[.]co/ODFwNI	X
17-May-23	@CollinSLKoh	https://southchinapost[.]net/WzMqB	X

Table 10: Tweets sent to target linked to Singapore.

DATE	TO	URL	PLATFORM
09-Feb-23	@thoibao_de	https://lnktonews[.]co/MEmK	X

Table 11: Tweets sent to target linked to Germany.

DATE	TO	URL	PLATFORM
12-Apr-23	@FMangosingINQ	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
12-Apr-23	@FMangosingINQ	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14-Apr-23	@FMangosingINQ	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
23-May-23	@FMangosingINQ	https://southchinapost[.]net/RtQBG	X

Table 12: Tweets sent to target linked to the Philippines.

DATE	TO	URL	PLATFORM
10-Apr-23	@ChinaDaily	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14-Apr-23	@ChinaDaily	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14-Apr-23	@ChinaDaily	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
12-Apr-23	@PdChina	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
26-May-23	@PDChinese	https://southchinapost[.]net/faePtONi	X
14-Apr-23	@SpotlightonCN	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X

Table 13: Tweets sent to targets linked to China.

DATE	TO	URL	PLATFORM
10-Apr-23	@Duandang	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X

Table 14: Tweets sent to target linked to Viet Nam.

DATE	TO	URL	PLATFORM
14-Apr-23	@jojjeols	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X

Table 15: Tweets sent to target linked to Sweden.

DATE	TO	URL	PLATFORM
10-Apr-23	@willripleyCNN @CNN @jimsciutto @EricCheungw	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
12-Apr-23	@GMFAsia	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X

Table 16: Tweets sent to targets linked to the United States.

DATE	TO	URL	PLATFORM
12-Apr-23	@Indopac_INFO	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
12-Apr-23	@Indopac_INFO	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14-Apr-23	@Indopac_INFO	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
14-Apr-23	@Indopac_INFO	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
17-May-23	@Indopac_INFO	https://southchinapost[.]net/WzMqB	X
22-May-23	@IMOSINT	https://southchinapost[.]net/fLwoASy	X
12-Apr-23	@ItsTheEnforcer	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X

Table 17: Tweets sent to OSINT-related accounts.

DATE	TO	URL	PLATFORM
12-Apr-23	@Manu_FAO	https://witteridea[.]co/LFJeZQu	X
16-May-23	@HugBallesteros	https://asean-news[.]net/HpjXXwRU	X

Table 18: Tweets sent to maritime or fisheries officials and researchers.

DATE	TO	URL	PLATFORM
8-Mar-23	@SariArhoHavren	https://lnktonews[.]co/CVqp	X
14-Mar-23	@SariArhoHavren	https://witteridea[.]co/mBxp	X
21-May-23	@ElBridgeColby	https://southchinapost[.]net/fLwoASy	X
12-Apr-23	@AsiaMTI	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14-Apr-23	@AsiaMTI @cnnphilippines	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14-Apr-23	@AsiaMTI	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
17-May-23	@GordianKnotRay	https://southchinapost[.]net/WzMqB	X

Table 19: Tweets sent to think tanks and researchers.

DATE	TO	URL	PLATFORM
08-Feb-23	@vitcheva_eu @EMODnet @cinea_eu @Pierre_Ka @EUgreenresearch @CMEMS_EU @FSUMDC @UNDPOceanInnov @REA_research @EU_ENV @EUClimateAction @eumissionocean	https://witteridea[.]co/LFJeZQu	X
08-Feb-23	@vitcheva_eu	https://witteridea[.]co/LFJeZQu	X
08-Mar-23	@GermanAmbUSA	https://Inktonews[.]co/CVgp	X
01-Jun-23	@EP_President	https://southchinapost[.]net/VuAfn	X
01-Jun-23	@EU_Commission	https://southchinapost[.]net/VuAfn	X
01-Jun-23	@EU_Commission	https://southchinapost[.]net/VuAfn	X
01-Jun-23	@eumissionocean	https://southchinapost[.]net/VuAfn	X

Table 20: Tweets sent to European officials and institutions.

DATE	TO	URL	PLATFORM
14-Apr-23	@iingwen @SenJohnHoeven	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
14-Apr-23	@MofaTaiwan @RepMcCaul	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X
22-May-23	@iingwen	https://southchinapost[.]net/RtQBG	X

Table 21: Tweets sent to senior U.S and Taiwan officials and institutions.

DATE	TO	URL	PLATFORM
1-Jun-23	@erionveliaj	https://southchinapost[.]net/eNISDKnI	X
1-Jun-23	@AlMissionEU @AlbanianDiplo	https://southchinapost[.]net/eNISDKnI	X
1-Jun-23	@AlMissionUNGen @AlbanianDiplo @AlEmbDenmark @AlMissionUN @AlMissionVienna	https://southchinapost[.]net/eNISDKnI	X
1-Jun-23	MirelaKumbaro	https://southchinapost[.]net/eNISDKnI	X
1-Jun-23	@GjonajEtilda @ChrisMurphyCT @GaryPeters	https://southchinapost[.]net/eNISDKnI	X
1-Jun-23	@MonicaMerino_D @AlbGob @MirelaKumbaro	https://southchinapost[.]net/eNISDKnI	X

Table 22: Tweets sent to Albanian officials and institutions.

DATE	TO	URL	PLATFORM
10-Apr-23	@AnarchoTerran	http://caavn[.]org/news/china/military/article/south-china-sea-pla-forcces-tail-us-warship	X
10-Apr-23	@MarioNawfal	http://caavn[.]org/news/china/article/us-defense-contractors-will-visit-taiwan	X

Table 23: Other Predator links shared to X accounts.

ANNEX III – ADDITIONAL PREDATOR LINKS SHARED ON SOCIAL MEDIA

DATE	TO	URL	PLATFORM
23-Mar-23	"Liën Minh Dân Chù"	http://caavn[.]org/tin-tuc/chien-su-ukraine	Facebook
23-Mar-23	"Liën Minh Dân Chù"	http://caavn[.]org/tin-tuc/quan-he-my-trung-sau-no-khi-cau	Facebook

Table 24: Links targeting a U.S-based Vietnamese political organisation.

ANNEX IV – ANALYSIS OF SUSPECTED ATTACKER RELATED SOCIAL MEDIA ACCOUNTS

Amnesty International analysed other accounts followed by or which follow the attacker-contolled '@Joseph_Gordon16' account. The X accounts followed by @Joseph_Gordon16 include multiple targeted accounts which later received Predator attack links.

Of the small number of accounts which follow @Joseph_Gordon16, many had an apparent interest in topics related to Viet Nam and cybersecurity. A number included profile pictures which were copied from a prominent Vietnamese businessman. Some of these accounts may be additional social media avatars linked to or controlled by the operator behind this campaign.

These followers of @Joseph_Gordon16 include the X account @bisngoo27345032, with a profile name Bí Ngô which translates from Vietnamese as "Pumpkin". This account followed multiple Vietnamese security researchers and cyber security companies based in Viet Nam. The account appears to have a keen interest in cybersecurity and new attack techniques.

Another follower of the @Joseph_Gordon16 account is @AlexMarcos71. This account states that it is based in the Philippines but follows a large group of Vietnamese accounts and also tweets in Vietnamese.

Figure 23: Profile of attacker-linked @ AlexMarcos21 account

Both the @AlexMarcos71 and @Joseph_Gordon16 X accounts sent tweets to an EU-based academic who researches illegal fishing with comments on the topic of the 'yellow card' issued to Viet Nam by the EU. The tweet from @Joseph_Gordon16 included a link to the Predator spyware.

@The @AlexMarcos71 account also tweeted about the "yellow card" system (see Figure 24) and sent a reply message mentioning the EU academic who was targeted with an attack link by @Joseph_Gordon16 (see Figure 25). The coordination between these accounts suggests that they are both controlled or managed by the operator behind this attack campaign.

Figure 24: @AlexMarcos71 account tweets in Spanish about the "Yellow Card" system

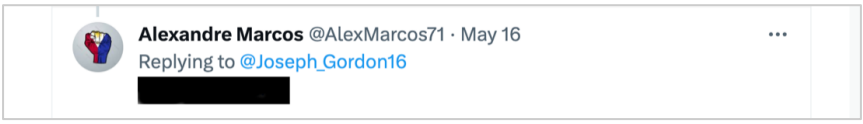


Figure 25: @AlexMarcos71 sends reply tweet mentioning Spanish academic target.

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.

CONTACT US


info@amnesty.org


+44 (0)20 7413 5500

JOIN THE CONVERSATION


www.facebook.com/AmnestyGlobal


@Amnesty

THE PREDATOR FILES: CAUGHT IN THE NET

THE GLOBAL THREAT FROM "EU REGULATED" SPYWARE

INDEX: ACT 10/7245/2023
OCTOBER 2023
LANGUAGE: ENGLISH

amnesty.org

AMNESTY INTERNATIONAL