AMNESTY INTERNATIONAL

TIGO IOR 40/9868/2019
22 February 2019

THE SURVEILLANCE INDUSTRY AND HUMAN RIGHTS

AMNESTY INTERNATIONAL SUBMISSION TO UNITED NATIONS SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION

INTRODUCTION

Amnesty International submits the following document in response to call for submissions[1] on the *Surveillance Industry and Human Rights.*

The international surveillance industry is unchecked. Existing standards, oversight and control mechanisms, such as the EU Dual Use Regulations, domestic export regulation and domestic courts,

[1] Call for Submissions: The Surveillance Industry and Human Rights, https://www.ohchr.org/Documents/Issues/Expression/SurveillanceIndustry/SurveillanceIndustry_HR.docx

are increasingly shown to be inadequate to prevent human rights abuses. States are not taking steps to introduce legislation to implement the due diligence steps laid down in the United Nations Guiding Principles on Business and Human Rights (UNGPs) for companies. These standards, systems and mechanisms do little to prevent surveillance related human rights abuses, nor to provide accountability when rights are violated. The consequences are dire for the security of human rights defenders (HRDs) and contribute to a quieting effect on civil society. Unchecked surveillance is yet another tool used by state and non-state actors to quiet HRDs and shrink civil society globally. Amnesty International therefore welcomes the upcoming report of your office and see it as a necessary step towards state and corporate accountability for abuses.

The international surveillance industry involves many actors: states, companies, third party ICT providers and more. It is truly an 'industry' because many states simply do not have the technical capacities to develop their own surveillance software, which creates a dependency on private corporations who specialize in making surveillance and interception software. What we see, though, is state collusion in keeping the surveillance industry hidden and covert. Even where systems are in place for the granting export licences for surveillance technology, states often fail to scrutinize the stated primary purpose of the surveillance tools - to fight crime and national security threats – and fail to take account of human rights abuses that the tools could facilitate. Covert surveillance is only justifiable when it is narrowly targeted based on reasonable suspicion, in accordance with the law, is strictly necessary to meet a legitimate aim (such as protecting national security or combatting serious crime) and is conducted in a manner that is proportionate to that aim and non-discriminatory.

We have documented the chilling effects of secret, mass surveillance, and see again and again cases of targeted surveillance of HRDs and civil society that are not prescribed by law, do not have a legitimate aim, and that fail the test of necessity, proportionality and non-discrimination. In this submission Amnesty International would like to highlight a number of problematic trends or characteristics of the international surveillance industry. Together these aspects of the surveillance industry create a dangerous environment for HRDs and civil society.

1) criminalization of human rights defence and human rights defenders;
2) targeted surveillance chills human rights regardless of infection;
3) export controls, surveillance technology and human rights;
4) lack of judicial oversight and lack of redress mechanisms;
5) superficial nods to due diligence frameworks;
6) cases: impact on HRDs and civil society.

This submission will go into the details of each of these trends and characteristics - highlighting the issues they present to HRDs and civil society and our recommendations for a human rights compliant system. The submission also includes a number of case examples that highlight the impact of the hidden yet ubiquitous nature of surveillance technologies, as well as the lack of accountability for privacy violations, and how this leaves civil society in a perceived panopticon; breaking trust networks and shutting down essential channels of communication.

1) CRIMINALIZATION OF HUMAN RIGHTS DEFENCE AND HUMAN RIGHTS DEFENDERS

The criminalization of human rights defenders is an important contextual framework for understanding the impact of the international surveillance industry. Targeted surveillance does not happen in a vacuum; it happens in a world where HRDs are increasingly being smeared as "criminals and terrorists".[2]

[2] In Saudi Arabia, authorities launched a smear campaign against six women human rights defenders, claiming they were part of a 'cell' posing a threat to national security. Amnesty International, *Saudi Arabia: Chilling smear campaign against women's rights defenders* (News: 19 May 2018) www.amnesty.org/en/latest/news/2018/05/saudi-arabia-chilling-smear-campaign-tries-

Criminalization can come about through active efforts by states, such as the enactment of repressive legislation, or by failing to update laws and/or adequately train law enforcement agencies. Therefore, from the perspective of the HRD, criminalization can take many forms, such as being accused of inciting violence, being targeted by excessively broad and vague legislation – especially counter-terrorism, anti-drug trafficking, national security and/or anti-extremism legislation – which is open to abuse. It also means that the catch-all justification of 'crime and terrorism' can be used by governments in very targeted ways towards HRDs. Some HRDs have their online accounts frozen and devices and digital information seized while judicial proceedings on spurious charges are ongoing.[3] Regardless of the formal outcome of criminal proceedings, the stigmatization and the diversion of energies and resources in fighting against these judicial attacks, can have hugely detrimental impacts on civil society.[4] It has an enormous impact on the HRD's ability to express themselves, complain, protest, communicate, and generally permits the closing of their space to do work.[5]

On one hand we have seen states increasingly criminalizing human rights work and on the other hand we have a surveillance industry that rebukes oversight with national security rhetoric. The result is an ever-widening chasm in which HRDs and civil society are caught; their human rights are violated, and they are left with nowhere to go for accountability or redress. The quieting effect of this is significant on HRDs and civil society, as will be demonstrated in the case studies.

2) TARGETED SURVEILLANCE CHILLS HUMAN RIGHTS REGARDLESS OF INFECTION

The existence of targeted surveillance powers can violate human rights regardless of whether targets are actively infected with malware, in the same way that the existence of unlawful mass surveillance systems creates a chilling effect on human rights.

Too often, states and others have attempted to downplay the threat posed to human rights by unlawful surveillance by arguing that such surveillance only threatens rights only when, in a system of unlawful mass surveillance, a person's communications or data are seen by a human, or in the case of targeted surveillance, when a target's device is actively infected with malware.[6]

This is incorrect. The surveillance technology for sale by private companies, which includes items such as monitoring centres and mobile telephone interception systems, has the possibility to enable both unlawful mass and targeted surveillance. As we posit here and further in the case study analysis, human rights may be violated from the mere existence of unlawful surveillance systems, not only with an active infection or viewing of data.

---

to-discredit-loujain-al-hathloul-and-other-detained-womens-rights-defenders/;
The Americas, including Mexico, has been touted as the most dangerous place to be a human rights defender in large part because of the criminalization defender face there. Amnesty International, *Americas: States must reverse rising tide of attacks against environmental human rights defenders* (News: 24 July 2018) www.amnesty.org/en/latest/news/2018/07/americas-states-must-reverse-rising-tide-of-attacks-against-environmental-human-rights-defenders/ ;
The experience of Francisca Linconao of Chile – a *machi*, or traditional Mapuche leader, from the Temuco area of southern Chile - who was wrongly prosecuted and charged on terrorism charges in an attempt to smear, discredit and make the public believe that she, and her network, were criminals. Amnesty International, *The criminalization of Indigenous leaders in Chile* (News: 23 April 2018) www.amnesty.org/en/latest/news/2018/04/la-criminalizacion-de-lideres-de-pueblos-indigenas-en-chile/

[3] Amnesty International, *Egypt: Asset freeze is a shameless ploy to silence human rights activism* (Press release, 17 September 2016) www.amnesty.org/en/latest/news/2016/09/egypt-asset-freeze-is-a-shameless-ploy-to-silence-human-rights-activism/

[4] Amnesty International, *Human Rights Defenders Under Threat: A Shrinking Space for Civil Society*, (Index: ACT 30/6011/2017) www.amnesty.org/en/documents/act30/6011/2017/en/

[5] Amnesty International, *Human Rights Under Surveillance: Digital Threats against Human Rights Defenders in Pakistan* (Index: ASA 33/8366/2018) www.amnesty.org/en/documents/asa33/8366/2018/en/ For more examples see FN 2.

[6] An active infection means a running device that was previously compromised and infected with a software implant that is currently still operational and able to collect and exfiltrate data.

This does not diminish the fact that cases of active surveillance are a significant threat for HRDs and civil society. The impact of such privacy breaches on other rights that are often concomitantly or subsequently violated as a result of those breaches can be especially harmful: for example, the right to freedom of expression;[7] the right to assemble peacefully; to seek, obtain, receive and hold information relating to human rights; and others, many of which are clearly articulated in the Human Rights Defenders Declaration.[8]

However, it should be noted that the lived reality for many defenders is that these subsequent violations occur regardless of whether an attempted digital attack results in infection or not. The fact that many systems of state surveillance are undertaken in secret, without adequate safeguards or remedies in place, means that for many HRDs, the lived reality of surveillance is one of never knowing whether they are subject to surveillance at any given moment, but knowing that they may be at any moment, and as a result, fearing to exercise their human rights.[9]

As our case studies document, HRDs frequently are forced to self-censor, to refrain from expressing political opinions over phone or email, or even in the privacy of homes, cars or offices, lest their legitimate activities give rise to prosecution, or otherwise end up being used against them. It is incorrect to assert – as some states do – that such self-censorship is not a violation attributable to the state. Rather, this self-censorship and other manifestations of chilling effects, are the direct and predictable result of state decision to purchase and deploy surveillance technology in a manner inconsistent with human rights law and standards, and are violations that are therefore squarely attributable to the actions of governments. Accordingly, companies should take account of the risk of such violations as part of their human rights due diligence.

In your report of May 2015, you noted that 'surveillance may undermine the right to form an opinion'.[10] Amnesty International believes this is true in cases where a HRD is targeted, even when it does not lead to a device infection. Being targeted by surveillance technology, even if the targeting does not lead to a compromised device, has a chilling effect on the right to freedom of expression and other related rights, and may cripple the ability of HRDs to carry out human rights work.[11]

An overly narrow conception of the human rights harms of surveillance, for instance one which is limited to cases of 'active infection' as the point where 'human rights harm' occurs, undermines the ability to seek legal accountability in cases involving unlawful targeted surveillance of HRDs and civil society. As such, human rights safeguards by states and companies must also account for the human rights threats that flow from the existence of unlawful surveillance regimes.

Recommendation

- States must ensure that surveillance powers are strictly in line with international human rights law and standards, and should be proactively transparent about the tools purchased or in possession.

[7] UNHRC, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye,* 22 May 2015, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

[8] OHCHR, *Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms,* www.ohchr.org/en/issues/srhrdefenders/pages/declaration.aspx

[9] See examples at footnotes 2 and 3

[10] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, 22 May 2015, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

[11] See footnotes 2 and 3

3) EXPORT CONTROLS, SURVEILLANCE TECHNOLOGY AND HUMAN RIGHTS

In principle, export controls may be a mechanism by which states can attempt to fulfil their human rights obligation to protect individuals against human rights abuses by third parties under their control, even if such abuses occur in other countries. At the same time, such controls can also assist companies in discharging their responsibilities to exercise human rights due diligence.

However, shortcomings in such export controls too often mean that they fail to achieve their ostensible core aim of protecting human rights in the context of surveillance exports. Indeed, since even well-crafted export controls are likely to be able – in isolation – to address all human rights concerns linked to surveillance exports, it is vital that they form only part of a more holistic approach that includes other avenues, including judicial, for redress and reparations for victims (see below).

Recast of the EU Dual-Use Regulation

One important initiative in this domain is the ongoing effort to recast the European Union's Dual-Use export regulation (Regulation (EC) No 428/2009).[12] Amnesty International has made detailed recommendations to this process,[13] but as the process is ongoing, it is not yet clear whether a revised regulation will be adequate to protect human rights in surveillance exports.

The European Commission released a proposal to update the dual-use regulation in September 2016.[14] The proposal itself contains several positive elements, including covering several new types of technology and requiring for the first time the taking into account of human rights in the granting of export licenses. However, it also has fundamental weaknesses, such as limitations in the catch-all to cover new technologies as they emerge, inadequate protections for internet security research, and the lack of requirement for transparency. Perhaps most urgently, the proposal contains an unduly narrow definition of human rights and fails to require that states deny licenses for surveillance exports that pose human rights risks.

The European Parliament adopted several amendments to the proposal that would at least partially address most of these concerns.[15] However, since then, leaked documents have indicated that a majority of EU member states are lobbying behind the scenes to significantly weaken key elements of the proposal that protect human rights.[16]

At present, the future of the legislative process is unclear in terms of whether the proposal will be revisited by the new incoming parliament and when the European Commission, Council and Parliament might engage in trialogue to negotiate a regulation.

Amnesty International and other members of CAUSE (The Coalition Against Unlawful Surveillance

---

[12] European Commission, *Commission proposes to modernise and strengthen controls on exports of dual-use items,* 28 September 2016, http://europa.eu/rapid/press-release_IP-16-3190_en.htm (hereinafter: European Commission, *Commission proposes to modernise and strengthen controls on exports of dual-use items)*

[13] Amnesty International Comments on the European Commission Dual-Use Export Proposal, April 2017, https://drive.google.com/file/d/0B69qfh7Q8vYyOTFPZjgwcTNGOVE/view. See also, Amnesty International, *Surveillance Exports : Time for the EU to Put its Money Where its Mouth is* (Op-ed: 11 May 2017) www.medium.com/amnesty-insights/surveillance-exports-time-for-the-eu-to-put-its-money-where-its-mouth-is-10b6cd3e4014

[14] European Commission, Proposal for a Regulation of the European Parliament and of the Council setting up a Union Regime for the Control of Exports, Transfer, Brokering, Technical Assistance and Transit of Dual-Use Items (recast), http://trade.ec.europa.eu/doclib/docs/2016/september/tradoc_154976.pdf

[15] Euractiv, *MEPs approve export controls tailored to stop government surveillance,* 17 January 2018, https://www.euractiv.com/section/cybersecurity/news/meps-approve-export-controls-tailored-to-stop-government-surveillance/

[16] Amnesty International, *EU : Leak reveals states are ready to put human rights defenders at risk to protect surveillance industry* (Press release: 29 October 2018) www.amnesty.org/en/latest/news/2018/10/eu-leak-reveals-states-are-ready-to-put-human-rights-defenders-at-risk-to-protect-surveillance-industry/

Exports), are urging that the final regulation must: require the denial of export licenses for surveillance exports that pose a substantial risk they could lead to human rights violations, require transparency in the licensing process, cover all surveillance technology, and protect security research and security tools.[17] A final regulation that fails to meet these criteria will be ineffective at preventing human rights abuses linked to surveillance exports.

Export Licences in Practice

Despite the inherently dangerous nature of surveillance products, export licences are still being issued to spyware companies to export their technology to states that have appalling human rights records. This is true even in countries that have export controls on surveillance technology, highlighting the need for further measures for states and companies to uphold human rights standards. The governmental department that issues the export licences varies across states, yet regardless of which bodies grant the licences, reports that surveillance tools have been used to target journalists, human rights defenders, and political dissidents, seem to go unheard as impunity reigns.[18] Victims of human rights abuses are unable to obtain redress as the due diligence processes that govern export licences are secretive and the considerations that governments take are largely unknown.

Even in countries that provide an element of transparency into licensing procedures, the limited information made public makes it difficult to scrutinize the adequacy of these procedures. Accordingly, much of what we do know comes from sources such as investigations by journalists. One such investigation found that over the three years leading up to 2017, EU states approved 317 export licenses for digital surveillance technology, with many of these exports ending up in countries with poor human rights records, including the United Arab Emirates—they denied only 14 licences.[19]

An example of how export controls can fail to protect human rights is NSO Group and the export licensing they receive under the Israeli Ministry of Defense (MOD). As will be examined through case examples below, when queried, the Israel MOD has maintained that the export licence issued to NSO Group is consistent with international obligations, regardless of the fact that its product, "Pegasus," was used to target an internationally recognized human rights organization and numerous other human rights defenders, journalists and parliamentarians around the world. This use goes far beyond legitimate aims such as fighting serious crime or preserving national security. There needs to be greater scrutiny of these processes.

At present, the authorities whose mandate include the issuing of these licences must do risk assessments to determine what is reasonably foreseeable in regard to human rights violations and abuses. This threshold however is not stringent enough because surveillance companies are continuing to sell their products to actors who repeatedly undermine human rights and use the technology to suppress expression and shrink civic space. On top of this, MOD due diligence processes are predominantly undisclosed, preventing accountability for human rights abuses that are a result of these surveillance exports.

Recommendations

- States should ensure that they have in place robust export licensing requirements for the sale of surveillance technology that, at a minimum:
    - Cover all existing and emerging surveillance technology;

[17] CAUSE, Shared Statement on the update of the EU dual-use regulation, May 2017, https://www.accessnow.org/cms/assets/uploads/2017/05/NGO_Sharedstatement_dualuse_May2017.pdf
[18] Amnesty International, *Amnesty International Among Targets of NSO-powered Campaign* (Research, 01 August 2018) https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/ (hereinafter: Amnesty International, *Amnesty International Among Targets of NSO-powered Campaign)*
[19] Sebastian Gjerding and Lasse Skou Andersen, De Correspondent, *How European Spy Technology Falls into the Wrong Hands*, 23 February 2017, https://thecorrespondent.com/6257/how-european-spy-technology-falls-into-the-wrong-hands/2168866237604-51234153

    - Requires denial of licenses for proposed exports with a substantial risk of harming human rights, including where legal safeguards are not in place to prevent abuse;
    - Protect internet security research and tools, and;
    - Mandate meaningful transparency regarding the consideration and grant or denial of licenses.
- Companies should have in place human rights due diligence processes which identify, prevent, mitigate and account for human rights impacts.
- Such export controls should form part of a larger package of measures aimed at ensuring that victims of surveillance technology have access to remedies and reparations, including through the courts.

4) LACK OF JUDICIAL OVERSIGHT AND LACK OF REDRESS MECHANISMS

Lack of remedies - OECD

The failure of states to investigate whether a company is able to ensure that its surveillance technology is not used to suppress human rights demonstrates the degree of impunity to which the surveillance industry operates. This is compounded by the difficulty in identifying which, if any, legal remedy to seek.

In 2013, Privacy International, among other organizations, filed a complaint against Gamma International UK Ltd[2021] when Gamma sold its surveillance software, FinFisher, to the Bahraini government whom have a history of human rights abuses. The Bahraini government then used the software to monitor HRDs. Research into this technology showed that it had been used to track individuals who were subsequently interrogated and tortured.[22] The claimants brought the complaint with the UK National Contact Point (NCP) for the OECD, alleging a breach of the OECD Guidelines for Multinational Enterprises. The OECD Guidelines contain a chapter on corporate respect for human rights which mirrors the corporate human rights responsibilities and due diligence provisions of the UNGPs.[23]

Though the UK NCP found that Gamma's conduct was inconsistent with its responsibilities under the OECD Guidelines, it was unable to confirm that Gamma caused or contributed to the human rights abuses alleged. Furthermore, the UK NCP was unable to verify that the human rights abuses complained of were directly linked to Gamma's business operations or relationships. This was because the NCP's mandate is limited to an information review, meaning that the boundaries set by the OECD Guidelines do not permit the NCP to force any party to provide information to it, nor obtain confidential information.[24] This meant that only if a criminal complaint is made can further information be investigated on the nature of the human rights violations.[25]

---

[20] Reporters Without Borders, *Summary of OECD Complaints*, rsf.org/sites/default/files/oecd_complaint_summary.pdf
[21] European Commission, *UK's OECD Guidelines Contact Point finds Gamma breached human rights by selling FinFisher spyware to Bahrain,* 9 March 2015 ec.europa.eu/digital-single-market/en/news/uks-oecd-guidelines-contact-point-finds-gamma-breached-human-rights-selling-finfisher-spyware
[22] Privacy International, *HMRC to go to trial over agency's refusal to reveal state of any investigation into Gamma International,* 9 February 2014 privacyinternational.org/press-release/1481/privacy-international-hmrc-go-trial-over-agencys-refusal-reveal-state-any
[23] Amnesty International, *Injustice Incorporated: Corporate abuses and the human right to remedy* (Index: POL 30/001/2014) www.amnesty.org/download/Documents/8000/pol300012014en.pdf, p. 21
[24] UK National Contact Point for the OECD Guidelines for Multinational Enterprises, *Privacy International & Gamma International UK Ltd: Final Statement after examination of complaint,* December 2014 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/402462/BIS-15-93-Final_statement_after_examination_of_complaint_Privacy_International_and_Gamma_International_UK_Ltd.pdf paras 26-27
[25] UK National Contact Point for the OECD Guidelines for Multinational Enterprises, *Privacy International & Gamma International UK Ltd: Final Statement after examination of complaint,* December 2014 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/402462/BIS-15-93-Final_statement_after_examination_of_complaint_Privacy_International_and_Gamma_International_UK_Ltd.pdf para. 74

Although positive in certain respects, the UK NCP decision falls far short of what would be needed to establish the full facts of the case and ensure accountability for the human rights violations experienced by Bahraini HRDs. In order to be able to substantiate a case of alleged complicity, the NCP relies solely on the corporation's own willingness to participate. If the company refuses to engage with the NCP, there remains a gap due to the limited mandate from the OECD Guidelines between knowing that there has been an attack and the ability to put together the evidence needed to ensure accountability.

Regardless of the inability to gain the information needed to establish a claim, the sheer lack of redress mechanisms prevents victims or organizations from taking action. Legal mechanisms are needed which go beyond voluntary mechanisms such as the OECD's NCP system and are able to investigate human rights abuses and hold accountable those found to be responsible.

Lack of remedies - Amnesty International

In June 2018, an Amnesty International staff member received a suspicious WhatsApp message with Saudi Arabia-related bait content and carrying links Amnesty International believes belong to infrastructure connected with "Pegasus", an exploit and surveillance tool built by Israeli-based NSO Group. Investigations by Amnesty International identified how these links are used to distribute and deploy this highly sophisticated and intrusive spyware.[26] NSO Group confirmed to us that it only sells its spyware tools to governments and government agencies and so presumably this digital attack was a deliberate attempt to infiltrate Amnesty International by a government hostile to our human rights work.[27]

Aside from the security as well as psychological implications this has had both on the staff member directly affected, and the pernicious chilling effect it has had on staff more generally at Amnesty International, several aspects of this attempted digital attack are demonstrative of the concerns submitted above. The brazenness of this attempted attack on one of the largest human rights organizations in the world underlines this fundamental culture of impunity in the surveillance industry. NSO Group maintains that its tool is only used "to identify and disrupt terrorist and criminal plots",[28] that each sale is advised on by a Business Ethics Committee and that they investigate any instances of misuse.[29] We are presently unclear about what actions NSO Group has undertaken in response to this targeting. NSO Group's response thus far has only suggested that they are either unable or unwilling to prevent its customers from misusing its powerful spyware tools.

Amnesty International wrote to the Israeli MOD on November 11, 2018 in order to request the revocation of the export license issued to NSO Group, in relation to the targeting of our staff member.[30] However in its response, the MOD stated that it does not provide information on the Israeli Government's policies of granting export licences or on the actual licences themselves, due to security, political and strategic grounds. Further, it stated that it cannot confirm nor deny the existence of the export licence, and that export licences issued by the Israeli MOD to NSO Group in relation to its government clients are consistent with international obligations.[31]

---

[26] Amnesty International, *Amnesty International Among Targets of NSO-powered Campaign*, 01 August 2018, https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/
[27] Amnesty International, *Amnesty International Among Targets of NSO-powered Campaign*, 01 August 2018, https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/
[28]Amnesty International, *Amnesty International Among Targets of NSO-powered Campaign*, 01 August 2018, https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/
[29] The Citizen Lab, *NSO Group statement*, 17 September 2018, https://citizenlab.ca/wp-content/uploads/2018/09/NSO-Statement-17-September-2018.pdf
[30] Amnesty International, *Israel: 'Rogue' NSO Group must have license revoked over controversial surveillance software,* (Press release: 28 November 2018) www.amnesty.org/en/press-releases/2018/11/israelroguenso-group-must-have-licence-revoked-over-controversial-surveillance-software/
[31] Letter of response received by Amnesty International from the Israeli Defence Export Control Agency (DECA), Ministry of Defence, 25 November 2018

There are a few troubling aspects of this response by Israel's MOD. The first is that there have been allegations made in an Israeli paper that a sale to Saudi Arabia of NSO Group's "Pegasus" technology was not authorized by the Israeli MOD.[32] If true, this suggests that the group has gone beyond the remit of the export licence granted by the Israel MOD.

As per the MOD's statement, we have no available evidence to suggest that robust human rights safeguards are included in the terms of export license issuance of surveillance technology, including of the particular licensing of the spyware "Pegasus". Moreover, the abovementioned allegations regarding a potential unsanctioned sale to Saudi Arabia also brings into question whether an export licence was even issued to NSO Group in relation to the government client that targeted our staff member.[33] We can therefore only conclude that either NSO Group sold its surveillance tool to its government client outside of the mandatory regulatory process; or, the Israeli MOD did issue NSO Group with an export licence but did not impose any robust human rights safeguard under the terms of its issuance. Ultimately, what is clear is that our request for the revocation of the export licence was unmet by the Israeli MOD and that, as a consequence, further attacks of the kind experienced by Amnesty International may occur.

It should also be noted that our request to the Israeli MOD was the second (known) request to the MOD to suspend or revoke NSO Group's export licence because of human rights abuses linked to the sale and use of their software by governments. In 2017, MK Tamar Zandberg, an Israeli politician, requested NSO's license be revoked after NSO's Pegasus was found to have targeted numerous HRDs, journalists and parliamentarians in Mexico. In this case, discussed below, the petition was taken to the Israeli Supreme Court. However, there is a gag order on the court ruling imposed on the petitioners and their legal counsel, which means that they are unable to comment publicly.

Recommendations

- The more vulnerable these surveillance tools are to politicised or improper use, the greater the threat it poses human rights. As such, states should ensure that authorities charged with overseeing the export of surveillance technologies have sufficient authority, independence and transparency to ensure adequate scrutiny of human rights risks.
- In addition, in order to realize their obligations under Article 2 ICCPR, states should also ensure that robust judicial or administrative oversight and redress mechanisms are in place to allow individuals to effectively vindicate their rights.

5) SUPERFICIAL NODS TO DUE DILIGENCE FRAMEWORKS

Regardless of state regulation and controls, companies have a responsibility to ensure through adequate due diligence steps that their surveillance technology is not used to suppress human rights.

The due diligence processes of surveillance companies such as NSO Group are opaque, creating an enormous hurdle in understanding how technology companies are, or are not, mitigating human rights risks. This is with regards to both general decisions to sell to governments with problematic human rights records or on more specific decisions related to individual targets.

NSO Group's response to any concerns raised with regards to their due diligence is that they have in

[32] A journalist received information that someone from within the Ministry claimed the sale to Saudi Arabia was unsanctioned. Haaretz, *Israeli Cyber Firm Negotiated Advanced Attack Capabilities Sale with Saudis, Haaretz reveals*, 25 November 2018 www.haaretz.com/israel-news/.premium-israeli-company-negotiated-to-sell-advanced-cybertech-to-the-saudis-1.6680618
[33] The Times of Israel, *Israeli hacking firm NSO Group offered Saudis cellphone spy tools - report*, 25 November 2018 www.timesofisrael.com/israeli-hacking-firm-nso-group-offered-saudis-cellphone-spy-tools-report/

place a Business Ethics Framework, and a Business Ethics Committee, which advises on each of their sales.[34] NSO Group have not made their Business Ethics Framework public. The fact that there have been repeated examples of human rights violations resulting from the sale and use of NSO Group's technologies indicate that the framework is either insufficient as per NSO Group's due diligence obligations and responsibilities, or that it is not being applied.

Similarly, NSO Group do not make any information public about the Business Ethics Committee. However as is clear from the numerous cases of alleged misuse of their tools, and the subsequent lack of redress, the existence of a Business Ethics Committee has not stopped sales to governments with poor human rights records, or at the very least, has not had any bearing on the individual human rights violations that occur from these sales. The lack of transparency about this Committee beyond confirmation of its existence has meant that Amnesty International are unclear on what the mandate of this Committee is, how they assess the risks associated with potential sales, and what bearing their conclusions actually have on NSO Group's activities.

On 28 November 2018, NSO Group publicly commented to Bloomberg that Amnesty International's accusations show that Amnesty International has no understanding "of the rigorous ethical and regulatory standards [they] abide by."[35] The company also told the Bloomberg reporter that if the company suspects misuse of its products, "NSO reserves the right to suspend or even terminate a contract". However, Amnesty International has seen no evidence that NSO Group has sought to recall its products or prevent further unlawful use of them. Given the complete lack of transparency about what these "ethical and regulatory" standards are, it is impossible to judge what human rights due diligence the company is currently doing.

What is clear is that either NSO Group's Business Ethics Committee's assessment is insufficient as per NSO Group's human rights due diligence obligations; or, NSO Group acts outside of the Committee's assessment; or, the Committee has less authority and influence over NSO Group's final sale decisions than the company claims.

The UNGPs state that, to meet their responsibility to respect human rights, companies should have an ongoing and proactive human rights due diligence process in place.[3637] This process should seek to identify and prevent, or mitigate, risks that their operations or products pose to human rights, with the aim of preventing human rights abuses.

It is not enough for businesses to be following the law where they operate. They must know their human rights impacts and take concrete steps to avoid causing or contributing to human rights abuses.[38] This means that, to meet their responsibility to respect human rights, companies might need to go beyond what is legally required in the jurisdiction.[39] When companies cause or contribute to human rights abuses, they have a responsibility to remediate the harm.[40] Companies should not exploit regulatory gaps or impede or stand in the way of victims seeking justice. The absolute non-

[34] The Citizen Lab, *NSO Group statement*, 17 September 2018, https://citizenlab.ca/wp-content/uploads/2018/09/NSO-Statement-17-September-2018.pdf
[35] Bloomberg, *Amnesty International Seeks Revocation of Israeli Spyware's Export License,* 28 November 2018 https://www.bloomberg.com/news/articles/2018-11-28/amnesty-seeks-revocation-of-israeli-spyware-s-export-license
[36] Human Rights Council, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, Report of the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, UN Doc A/HRC/17/31, 21 March 2011, https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf (hereinafter: Human Rights Council, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework)
[37] Human Rights Council, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, Report of the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, UN Doc A/HRC/17/31, 21 March 2011. Principle 15(b). The steps of the suggested human rights due diligence process are elaborated further in Principles 17 to 21.
[38] Amnesty International, *Injustice Incorporated: Corporate abuses and the human right to remedy* (Index: POL 30/001/2014) www.amnesty.org/download/Documents/8000/pol300012014en.pdf
[39] Human Rights Council, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. Principle 11 and Commentary.
[40] Human Rights Council, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, Principle 22.

transparency of due diligence processes in surveillance companies undermines the ability of victims to scrutinize their conduct, hold them accountable and access remedy.

Despite much talk of progress, companies are still overwhelmingly failing to adopt and implement robust human rights due diligence processes. Governments, on their part, are also largely failing to adopt effective laws and regulations to ensure companies undertake adequate human rights due diligence. These protection and accountability gaps are particularly severe in relation to the surveillance industry.

Recommendations

- To help meet the obligation to regulate the conduct of non-state actors who are under their control in order to prevent them from causing or contributing to human rights harms, even if they occur in other countries, states should take legislative and other measures to ensure that companies meet their human rights due diligence responsibilities.
- The UNGPs require that companies take pro-active steps to ensure that they do not cause or contribute to human rights abuses within their global operations, and to respond to any human rights abuses when they do occur. This corporate responsibility to respect human rights 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. 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".

6) CASES: IMPACT ON HRDS AND CIVIL SOCIETY

The narrative consistently spun by government and non-government actors to justify the sale, export and use of spyware tools is that these dual-use weapons shall be only targeted at 'criminal' and 'terrorist' entities in order to disrupt 'criminal' and 'terrorist' plots.[41]

However as is increasingly becoming clear, an alarming number of targets of such digital attacks are in fact HRDs, civil society and human rights organizations.[42] This reality becomes significantly more problematic given, as aforementioned, the increasing criminalization of human rights activism as a way to intimidate activists and crackdown on the right to freedom of opinion and expression, as well as peaceful dissent.

With this context, the plausibility of spyware tools being misused against HRDs and civil society, along with actual documented cases, and insufficient regulatory frameworks and safeguards makes clear that the resultant infringement of human rights and the serious lack of effective accountability mechanisms are inconsistent with the international obligations of states as well as due diligence obligations of companies.

As such, the cases outlined in this section collectively illustrate not only the chilling effects of unlawful surveillance, but also multiple cases of the misuse of highly sophisticated spyware against HRDs and civil society, including the premeditated nature of these digital attacks. Furthermore, and most significantly, these cases are only a few of those that have been exposed. Core to the surveillance industry is the undetectability of its spyware tools and therefore this begs the question, how many other HRDs and member of civil society have actually received such attacks?

[41] For example, NSO Group states that its tools "is intended to the be used exclusively for the investigation and prevention of crime and terrorism". Amnesty International, *Amnesty International Among Targets of NSO-powered Campaign*

[42] For example, it was revealed that the UK government subjected two NGOs, including Amnesty International, to mass surveillance: Amnesty International, *UK surveillance Tribunal reveals the government spied on Amnesty International,* (Press release: 1 July 2015) www.amnesty.org/en/latest/news/2015/07/uk-surveillance-tribunal-reveals-the-government-spied-on-amnesty-international/

Case: Chilling Effects of Surveillance in Belarus

The legal framework governing secret surveillance in Belarus is characterized by inadequate safeguards, and allows the authorities to undertake wide-ranging surveillance with little or no justification.[43] The surveillance tools available to the government include widespread passive surveillance via the SORM system,[44] and likely tools for targeted attacks as well.[45] Leaked documents from 2015 appear to show state agents attempting to purchase software from the Italian company Hacking Team. It is not known whether this sale was completed or what other surveillance tools the government may have acquired from private companies.[46]

While it is possible that almost anyone in Belarus could be subject to surveillance, it is nearly impossible for anyone to know whether they are or have been. This uncertainty exerts a chilling effect on human rights defenders, opposition politicians, lawyers and activists, and limits their ability to exercise their human rights, including the rights to privacy, freedom of association, peaceful assembly and expression.

Activists and journalists in Belarus told Amnesty International how the widespread fear of surveillance makes it nearly impossible for them to carry out daily activities like sending emails, making phone calls or organizing meetings.

This is compounded by laws that criminalize basic freedoms like holding unauthorized protests, As a result, their ability to exercise their human rights and to participate in the political life of the country is severely curtailed.

One Belarusian activist told us: "In principle if I am talking indoors, or on the phone, or writing emails, I assume it all gets to the KGB."

It bears emphasizing that much of the harm that flows from systems of secret, unlawful surveillance like that in Belarus comes from the uncertainty that surrounds them. Even the threat of surveillance can have a chilling effect.

Activists in Belarus jokingly refer to mobile phones as "the police officer in your pocket." You cannot know whether your phone is tracking you or listening to you – but it could be.

One Belarusian activist noted that in order for civil society to be kept in check, the government need not resort to jailing people or threatening them. With surveillance, "it's enough for people to feel it exists."

Case: NSO Group Assault on Civil Society

Examining instances where malicious digital attacks connected to NSO Group's spyware infrastructure were found - just one company amongst numerous spyware companies that form the surveillance industry - illustrates a history of abuse despite claims by NSO Group that their products

---

[43] Amnesty International, "Belarus: 'It's Enough for People to Feel it Exists': Civil Society, Secrecy and Surveillance in Belarus," July 2016, https://www.amnesty.org/download/Documents/EUR4943062016ENGLISH.PDF

[44] "SORM" is the English abbreviation for the **система технических средств для обеспечения оперативно- розыскных мероприятий** (or **СОРМ**) - a set of standardized technical means for interception of communications and associated data. SORM first appeared in Russia and versions now exists in many countries of former USSR, including Belarus, where it provides state authorities with direct, automated access to communications and associated data from communications providers, including landline telephones, mobile networks and internet service providers (ISPs).

[45] Amnesty spoke to several activists who appear to have been subjects of targeted digital attacks, often leading to legal consequences.

[46] OOCRP, *Belarus Wanted To Use USB Sticks to Infect Devices and Collect Data*, 15 July 2015, https://www.occrp.org/en/daily/4161-belarus-wanted-to-use-usb-sticks-to-infect-devices-and-collect-data ; Charter 97, *OAC interested in DaVinci spyware,* 16 July 2015, https://charter97.org/en/news/2015/7/16/160052/

are not used for nefarious purposes. This forms a case study illustrating several of the concerns and gaps discussed, whereby NSO Group's surveillance tools have been repeatedly misused by government clients against HRDs and civil society without accountability.

Targeting of a HRD from the United Arab Emirates

Ahmed Mansoor

- Prominent HRD from the United Arab Emirates.
- In 2016, he was found to have been targeted with NSO Group's Pegasus spyware after having previously been targeted at least twice with spyware developed by German-British Gamma Group and Italian Hacking Team.[47]

The first discovery of Pegasus spyware was made possible due to Ahmed Mansoor's proactive sharing of the malicious content he received with Citizen Lab who investigated and confirmed this.[48] Mr. Mansoor's actions meant that numerous other instances of digital attacks involving Pegasus were identifiable and that the human rights movement were aware of some indicators of Pegasus attacks.

Yet since his arrest in March 2017, he has been subjected to a prolonged period solitary confinement and was later convicted and sentenced to 10 years in prison and fined 1,000,000 Emirati Dirham in May 2018, for posts he made on social media in connection with his human rights work.[49]

Targeting of Mexican HRDs, journalist and lawyers

- In 2015 reports exposed an expansive surveillance campaign that targeted at least 24 Mexican HRDs, lawyers and journalists - including a minor.[50]
- In 2017 a federal Investigation into abuses associated with NSO Group's spyware was opened by the Mexican government, however according to reports, the investigation has stalled.[51]
- Also in 2017, despite the revelations and fallout that resulted from the events in 2015, the Pegasus tool was reported to be used again against a Mexican journalist, Javier Valdez Cárdenas, days before his assassination in Mexico. Days later a close colleague of Mr. Cárdenas was targeted with a suspicious message that claimed to have information on Mr. Cárdenas' assassins - according to reports, had the link contained within the message been opened, it would have also delivered a Pegasus infection.[52]
- Presently, NSO Group are at the centre of twin lawsuits in Israel and in Cyprus filed by a Qatari citizen and Mexican journalists for its sale of Pegasus spyware to the Mexican government as well as allegations of NSO Group being improperly involved in targeting demonstrations for the UAE government.[53]

---

[47] The Citizen Lab, *Backdoors are forever*, 10 October 2012, https://citizenlab.ca/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/

[48] The Citizen Lab, *The Million Dollar Dissident*, 24 August 2016, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

[49] Amnesty International, *UAE: 10-year prison sentence upheld for prominent human rights defender Ahmed Mansoor* (News, 31 December 2018) www.amnesty.org/en/latest/news/2018/12/uae-10-year-prison-sentence-upheld-for-prominent-human-rights-defender-ahmed-mansoor/

[50] The New York Times, *Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families*, 19 June 2017 www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html?module=inline ; The Citizen Lab, *RECKLESS EXPLOIT: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware*, 19 June 2017, https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/

[51] The New York Times, *Mexico Spyware Inquiry Bogs Down. Skeptics Aren't Surprised.*, 20 February 2018, https://www.nytimes.com/2018/02/20/world/americas/mexico-spyware-investigation.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news&mtrref=undefined

[52] The Citizen Lab, *Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague*, 27 November 2018 https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/

[53] The New York Times, *Hacking a Prince, an Emir and a Journalist to Impress a Client*, 31 August 2018,

The 2015 case saw a high-level Mexican journalist targeted with messages impersonating the United States Embassy in Mexico. This illustrates a problematic and potentially criminal trend also seen in other cases where attackers fraudulently impersonate government bodies in order to bait targets into opening suspicious messages containing spyware or credential attacks.

Moreover, the targeting in the 2015 case of a minor who was related to another target serves as another example of how these campaigns can affect and impact those who are closest to the primary victim.

Another problematic trend visible in the 2017 case was attackers baiting targets with messages claiming to have information about at-risk colleagues. This trend was also observed in other cases including the case of a HRD who was targeted with credential phishing and malware in Pakistan.[54]

Targeting of an Amnesty International staff member

Amnesty International

- In June 2018, an Amnesty International staff member was targeted with a suspicious message containing a link that we believe would have distributed and deployed potent spyware that overlaps with the Pegasus' tool's infrastructure.
- While investigating this, we uncovered over 600 domains linked to infrastructure that overlaps with NSO Group's Pegasus infrastructure – each of these domains represent potential threats to HRDs and civil society in countless other countries around the world.[55]

In terms of the impact that the targeting of an Amnesty International staff member has had on the movement, we witnessed concern and disbelief at its brazenness. The targeting of our staff member in order to infiltrate and surveil our human rights work is an attack on us, a prominent global human rights movement. Again, it serves as a reminder of the culture of impunity attached to the surveillance industry that permits actors to determine that targeting an organization like Amnesty International at the risk of getting caught and exposed is still not a risk big enough to deter such conduct, for there is no expectation that accountability will be successfully sought.

Internally, we have had to reinforce the online and offline security of our staff members and increase the scope of our security processes relating to our staff to firmly include digital attacks. The widespread rise of digital attacks being received by HRDs and civil society across the world as well as our own targeting only evidences how digital attacks of this nature are becoming common tools of repression and intimidation. This attack has only made us more committed to ending the human rights violations that are increasingly becoming synonymous with this kind of targeted hacking and surveillance operations.

Targeting of Saudi Arabian dissidents in the United Kingdom and Canada

Yahya Assiri

- Saudi Arabian activist currently residing in the United Kingdom.
- Coinciding with the targeting of an Amnesty International staff member, Mr. Assiri also received similar digital attacks.[56]

---

https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html

[54] Amnesty International, *Human Rights Under Surveillance: Digital Threats against Human Rights Defenders in Pakistan* (Index number: ASA 33/8366/2018)

[55] Amnesty International, *Amnesty International Among Targets of NSO-powered Campaign*, 01 August 2018, https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/

[56] Amnesty International, *Amnesty International Among Targets of NSO-powered Campaign*, 01 August 2018, https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/. This publication anonymises Yahya Assiri; however, Mr. Assiri later publicly disclosed his identity as the Saudi Arabian activist referenced in Amnesty International's report.

Omar Abdulaziz

- Saudi Arabian activist currently residing in Canada.
- In summer 2018 Mr. Abdulaziz also received a malicious link connected to the Pegasus infrastructure.[57]
- In December 2018 Mr. Abdulaziz filed a lawsuit in Israel against NSO Group which alleges that the spyware he received was used by Saudi Arabia to spy on his conversations with the late Jamal Khashoggi. [58]

Both Mr. Assiri and Mr. Abdulaziz have noted that they were in frequent contact with the late Jamal Khashoggi before he was murdered in October 2018.[59] A case that cannot highlight any more clearly that targeted surveillance of HRDs and journalists can come to dire ends.

While it could be speculated that there is a connection and even in some cases potential overlap between the identities of the government clients behind some of these attacks, the known recurrent actor is NSO Group and as of present, there has been no known meaningful redress of these violations by either NSO Group, the Israeli MOD as its exports licensing authority, or any of the government clients involved.

This is in spite of multiple lawsuits which have been filed against NSO Group, including by Mr. Abdulaziz in December 2018. Mr. Abdulaziz alleges that the spyware was used to monitor and spy on his conversations with Mr. Khashoggi – which Mr. Abdulaziz believes "played a major role in what happened to Jamal [Khashoggi]".[60] This lawsuit runs parallel to the aforementioned twin lawsuits against NSO Group filed by a Qatari citizen and Mexican journalists.[61] Similarly, previous lawsuits have been filed calling upon the Israeli Ministry of Defense to revoke NSO Group's licence.[62]

Charting cases associated with just one company amongst numerous others that constitute the surveillance industry, we find that cumulatively they evidence that while NSO Group sells its co-called "lawful interception" tools to governments ostensibly to fight serious crime and terrorism, in practice their spyware is undoubtedly being used to repress the legitimate activities of civil society.

Case: Campaign of hacking, spyware and surveillance targeting HRDs in Pakistan

A WHRD who was amongst the HRDs targeted by this campaign

- Prominent peace activist who had been campaigning for the release of a colleague that had been 'forcibly disappeared'. She was also the petitioner in the case calling for his release.
- In late 2016, the WHRD began receiving first contact from fake profiles on social media. The fake profiles began communicating with the WHRD in order to develop trust with her.
- From December 2017 till March 2018, these fake profiles sent the WHRD suspicious messages containing different kinds of spyware and credential phishing attacks.
- In December 2017 the WHRD received the first visit at her office by a person claiming to

[57] The Citizen Lab, *The Kingdom came to Canada*, 1 October 2018, https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/
[58] NPR, *Khashoggi Friend Accuses Cyber Security Firm of Helping Saudis Spy On Their Messages*, 3 December 2018 www.npr.org/2018/12/03/673105423/khashoggi-friend-accuses-cyber-security-firm-of-helping-saudis-spy-on-their-mess?t=1549540160137
[59] The Washington Post, *Secret recordings give insight into Saudi attempt to silence critics*, 17 October 2018 https://www.washingtonpost.com/world/secret-recordings-give-insight-into-saudi-attempt-to-silence-critics/2018/10/17/fb333378-ce49-11e8-ad0a-0e01efba3cc1_story.html?utm_term=.f901b190d4ff
[60] NPR, *Khashoggi Friend Accuses Cyber Security Firm of Helping Saudis Spy On Their Messages*, 3 December 2018 www.npr.org/2018/12/03/673105423/khashoggi-friend-accuses-cyber-security-firm-of-helping-saudis-spy-on-their-mess?t=1549540160137
[61] The New York Times, *Hacking a Prince, an Emir and a Journalist to Impress a Client*, 31 August 2018, www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html
[62] See for example, this ongoing Israeli civil law suit against NSO Group filed in 2018 (in Hebrew). https://www.documentcloud.org/documents/4806664-NSO-Lawsuit-in-Hebrew.html The documents were leaked online and publicly shared by members of the press. See https://twitter.com/razhael/status/1035652638547816448

be one of the fake profiles. This person signed the guest register with the name of the fake profile but provided the phone number of the WHRD.
- In January 2018 the WHRD received the second visit at her office by the same person claiming to be the fake profile. This time they again sign they guest register with the name of the fake profile, however they leave a scribble where they needed to indicate phone number.
- Also in March 2018, the WHRD received an email claiming to be from government officials and relating to the 'enforced disappearance' of her colleague – this email contained malware.

Digital presence, particularly online communications through email, messaging services and even social media, is increasingly central to progressing human rights work and yet it is those digital tools of freedom that are being purposefully exploited by hostile states. The sophistication of techniques used to bait targets with phishing links now include social engineering. Amnesty International's investigation into the surveillance of HRDs in Pakistan is an example of this baiting and involved gathering intelligence from and about victims via social media and other social forums in order to tailor digital attacks in a way that baits the victim to engage. [63]

This report in particular highlighted how online monitoring and harassment can permeate the offline realm, with one of the HRDs referenced in the report receiving visits to their office from a person claiming to be the fake social media profile that contacted them.[64] Further, the investigation also revealed how attacks even impersonated staff of the Chief Minister of Punjab province. The emails included false details of a supposed upcoming meeting between the provincial Ministry of Education and the victim's human rights organization.

For the WHRD who was the target of these attacks the impact was significant. Not only did she have to leave her home country - thereby effectively thwarting her activism - but she became worried that all communications, even emails from families, were attempts to spy on her. In the words of the WHRD herself, "every time I open an email I am now scared. It's getting so bad I am actually not able to carry out my work – my social work is suffering."[65]

Case: Targeting of HRDs, journalists and political activists in Azerbaijan

Rasul Jafarov
- Prominent lawyer, HRD, and former Amnesty International prisoner of conscience who had previously spent more than a year and a half in prison on trumped-up, politically motivated charges stemming from his human rights work.
- In October 2016 Mr. Jafarov received a phone call from a colleague warning him that they had been sent an email and attachment from an address very similar to Mr. Jafarov's email address.[66]
- This was one case amongst several caught up in this campaign of digital attacks.

This case was uncovered as part of research carried out by Amnesty International that revealed how HRDs, journalists and political activists in Azerbaijan - most of whom were critics of the government - were targeted by a fraudulent and sustained 'spear phishing' campaign using emails and Facebook

[63] Amnesty International, *Human Rights Under Surveillance: Digital Threats against Human Rights Defenders in Pakistan* (Index number: ASA 33/8366/2018)
[64] Amnesty International, *Human Rights Under Surveillance: Digital Threats against Human Rights Defenders in Pakistan* (Index number: ASA 33/8366/2018) p. 23
[65]Amnesty International, *Pakistan: Campaign of hacking, spyware and surveillance targets human rights defenders* (News: 5 May 2018) www.amnesty.org/en/latest/news/2018/05/pakistan-campaign-of-hacking-spyware-and-surveillance-targets-human-rights-defenders/
[66] Amnesty International, *False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan* (Op-ed: 09 March 2017) https://medium.com/amnesty-insights/false-friends-how-fake-accounts-and-crude-malware-targeted-dissidents-in-azerbaijan-9b6594cafe60

chat, aimed at gaining access to their personal information and private communications.[67] If the recipient of the email clicked on the attachment, a virus would download, relaying images of the target's screen back to the attacker and enabling them to record what the target typed. These emails were mostly sent from addresses impersonating prominent human rights and political activists. In another incident, malware was sent to several activists disguised as an invitation for a reception at the US Embassy in Baku.

The chilling suggestion that online activity is potentially being monitored created unease among activists in Azerbaijan, undermining their vital work, and also had serious impacts on their day-to-day lives. Turgut Gambar, a youth activist in Azerbaijan, told Amnesty International how "in regards to surveillance there is a feeling in society and with the activists that everyone is watched all the time...People are trying to be not quite open during their online communication. People prefer to meet face to face because of this atmosphere of fear. It creates some level of paranoia as well". Even those HRDs who have left Azerbaijan, like Leyla and Arif Yunus who now live in The Netherlands, are affected. Ms. Yunus' email was also impersonated as part of the campaign, and her computer was discovered to have been compromised by the malware used in that campaign. She worried that this had put those whom she communicated with at risk: "...if this virus reads what we write in our messages and makes it possible to identify those who we talk to, it poses a threat not just to us, but to our colleagues, our friends".[68]

These case studies are only a few of those exposed and yet they cumulatively portray an alarmingly bleak image of the current reality of the surveillance industry. Insufficient regulation, lack of transparency, unchecked targeting of HRDs and civil society in order to harass, intimidate, repress and ultimately silence them, a lack of accountability and effective redress mechanisms - these are all longstanding challenges faced by the human rights movement. As this submission has made clear, these same challenges have simply transcended into the digital realm with devastating online and offline consequences for those affected. As such, while this submission identifies serious issues in various aspects of the surveillance industry, it also posits the urgent need for effective, collaborative and meaningful responses and action.

[67] Amnesty International, *False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan* (Op-ed: 09 March 2017) https://medium.com/amnesty-insights/false-friends-how-fake-accounts-and-crude-malware-targeted-dissidents-in-azerbaijan-9b6594cafe60

[68] Amnesty International, *False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan* (Op-ed: 09 March 2017) https://medium.com/amnesty-insights/false-friends-how-fake-accounts-and-crude-malware-targeted-dissidents-in-azerbaijan-9b6594cafe60