Human Rights Organizations' Response to the Adoption of the New EU Dual Use Export Control Rules

March 2021

Human Rights Organizations's Statement in Response to the Adoption of the New EU Dual Use Export Control Rules

We, the undersigned organisations, welcome the positive elements adopted by the EU legislators to reform the European Union's Dual Use Regulation aimed at preventing human rights harm resulting from digital surveillance by establishing export controls for surveillance technology exported by EU-based companies. At the same time, the overall resulting agreement is a missed opportunity for a more ambitious regulation that includes stronger protections needed to safeguard human rights and security.

While certain positive elements of the compromise agreement are welcome, including the requirement for EU authorities to provide publicly detailed information about which export licenses have been approved or denied and the human rights risks associated with the applications for export licenses by companies, the agreement falls short of providing explicit and strong conditions on Member State authorities and exporters. These conditions have been voiced to the EU legislature many times. It is evident that while some parliamentarians and Member States have recognised the need for greater protections throughout negotiations, other Member States have prioritised the narrow interests of industry over their obligations to protect human rights.

It should not have taken almost a decade of lawmaking to finalize this process. As negotiations stalled and the stronger provisions in the original Commission's proposal were watered down,[1] EU-based companies have continued to undermine people's human rights by selling and exporting surveillance technology around the world, including into the hands of known rights abusers. Further, vital measures that would have placed meaningful constraints on the export of dual use technology were not agreed upon (see analysis below).[2]

However, now, it is vital that all Member States robustly implement the positive elements of the agreement. EU Member States and the Commission also need to go further than the new compromise in order to meet their international human rights obligations and ensure that the continued export of sophisticated surveillance tools by EU companies does not facilitate human rights violations of people around the world.

The Commission should expeditiously develop in consultation with civil society, clear guidelines to ensure adherence to the new measures and disseminate them among all national and business stakeholders. Most importantly the Commission should closely monitor Member States'

[1] "EU member states are watering down spyware regulation" (Access Now, 15 November 2018) https://www.accessnow.org/eu-member-states-are-watering-down-spyware-regulation/; "Human rights organizations call to strengthen the European Commission position on dual-use recast" (Access Now, 9 June 2020) https://www.accessnow.org/human-rights-organizations-call-to-strengthen-the-european-commission-position-on-dual-use-recast/.

[2] "Urgent call to Council of the EU: human rights must come first in Dual Use final draft" (Access Now, 5 November 2020) https://www.accessnow.org/urgent-call-to-council-of-the-eu-human-rights-must-come-first-in-dual-use-final-draft/.

implementation of the new regulation, and adopt all necessary measures under EU law to prevent, discipline, and remedy any possible breach that may occur.

Background

Since our first calls for reforms to the Dual Use Regulation in 2011 in the midst of the Arab uprisings, the Parliament and some Member States have consistently called on the Commission to take urgent steps to reform the regulation to control the export of surveillance technology.

In September 2016, the Commission proposed positive changes to "prevent human rights violations associated with certain cyber-surveillance technologies," by enacting appropriate human rights standards.[3] On 23 November 2017, the European Parliament's International Trade Committee (INTA) also voted on a promising proposal to implement stronger dual use rules.[4] However, progress has been continuously undermined by Member States and industry groups unwilling to impose strong, binding commitments on corporate actors and export control authorities.[5] These new rules reflect the final compromise between the Parliament and Member States.

During the period of lawmaking, EU-based surveillance companies have continued to export surveillance technology to destinations in which human rights defenders, journalists, and minority groups are targeted by surveillance in violation of international human rights law. Since the beginning of negotiations, it has been reported that:

- Three companies based in France, Sweden, and the Netherlands sold digital surveillance systems, such as facial recognition technology and network cameras, to key players of the Chinese mass surveillance apparatus;[6]
- Software sold by Germany-based spyware merchant FinFisher was used to target the main opposition party in Turkey during a protest, and was also found in Myanmar and Egypt;[7]

[3] "Commission proposes to modernise and strengthen controls on exports of dual-use items" (28 September 2016) http://trade.ec.europa.eu/doclib/press/index.cfm?id=1548.
[4] "The European Parliament is fighting to strengthen the rules for surveillance trade" (Access Now, 8 Decemebr 2017) https://www.accessnow.org/european-parliament-fighting-strengthen-rules-surveillance-trade/.
[5] "EU member states are watering down spyware regulation" (Access Now, 15 November 2018) https://www.accessnow.org/eu-member-states-are-watering-down-spyware-regulation/.
[6] "EU companies selling surveillance tools to China's human rights abusers" (Amnesty International, 21 September 2020) https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers/.
[7] "New report: FinFisher changes tactics to hook critics" (Access Now, 14 May 2018) https://www.accessnow.org/new-report-finfisher-changes-tactics-to-hook-critics/; "New versions of FinFisher mobile spyware discovered in Myanmar" (ZDNet, 10 July 2019) https://www.zdnet.com/article/new-versions-of-finfisher-mobile-spyware-discovered-in-myanmar/; "German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed" (Amnesty International, 25 September 2020) https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/.

- The Colombian Army used a platform sold by a Spanish company, Mollitiam, to spy on senior judges, politicians, and journalists;[8]
- According to an investigation by *The Correspondent*, 17 Member State authorities approved at least 317 licenses for exports of controlled surveillance technology between 2014-2017 and denied only 14;[9]
- According to the European Commission in 2017 alone, 285 licenses for exports of controlled surveillance technology were approved across the EU while only 34 were denied. The Member States are not specified because this information is not subject to transparency mechanisms;[10]
- BAE Systems received export licenses for mass internet surveillance systems from authorities in Denmark and the UK, including to countries with bad track records on human rights and surveillance such as Saudi Arabia, the United Arab Emirates (UAE), Qatar, and Morocco;[11]
- Two French companies, Ercom and Nexa, sold internet surveillance equipment to Egyptian authorities which are known for their track record of human rights violations with surveillance;[12]
- Finnish authorities approved the export of 80 licenses for telecommunications interception equipment between 2015 and 2017, including to Morocco, Colombia, the UAE, and North Macedonia, all destinations in which there is considerable evidence that authorities have monitored human rights defenders;[13]
- German authorities approved more than €26 million worth of exports of surveillance equipment, including to Egypt, Qatar, Saudi Arabia, and the UAE between 2015-2019;[14]
- Italy-based Hacking Team sold spyware to Ethiopia, Bahrain, Egypt, Kazakhstan, Morocco, Russia, Saudi Arabia, Sudan, Azerbaijan, and Turkey;[15] and

---

[8] "Investigation reveals corruption and illegal interceptions by the Colombian Army" (Al Dia News, 15 January 2020) https://aldianews.com/articles/politics/investigation-reveals-corruption-and-illegal-interceptions-colombian-army/57348.

[9] "How European spy technology falls into the wrong hands" (The Correspondent, 23 February 2017) https://thecorrespondent.com/6257/how-european-spy-technology-falls-into-the-wrong-hands/2168866237604-51234153.

[10] "Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, including a report on the exercise of the power to adopt delegated acts conferred on the Commission pursuant to Regulation (EU) No 599/2014 of the European Parliament and the Council of 16 April 2014 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual use items" (4 Novermner 2019) https://ec.europa.eu/transparency/regdoc/rep/1/2019/EN/COM-2019-562-F1-EN-MAIN-PART-1.PDF.

[11] "How BAE sold cyber-surveillance tools to Arab states" (15 June 2017), https://www.bbc.co.uk/news/world-middle-east-40276568.

[12] "Amesys: Egyptian trials and tribulations of a French digital arms dealer" (Télérama, 8 Decmeber 2020) https://www.telerama.fr/monde/amesys-egyptian-trials-and-tribulations-of-a-french-digital-arms-dealer,160452.php; "On a encore trouvé une société française qui vend du matériel de surveillance électronique à l'Egypte" (Télérama, 26 March 2018) https://www.telerama.fr/monde/on-a-encore-trouve-une-societe-francaise-qui-vend-du-materiel-de-surveillance-electronique-a-legypte,n5533721.php.

[13] "New Data Gives Peek at European IMSI Catcher Exports" (Vice, 23 March 2018) https://www.vice.com/en/article/wj75yq/imsi-catcher-exports.

[14] "EU will Export von Späh-Programmen an Diktatoren stoppen" (Handelsblatt, 7 November 2020) https://www.handelsblatt.com/technik/it-internet/ueberwachungstechnologie-eu-will-export-von-spaeh-programmen-an-diktatoren-stoppen/26598522.html?ticket=ST-11857895-LebLXK4AOoMmWLP2hLL7-ap1.

[15] "A Detailed Look at Hacking Team's Emails About Its Repressive Clients" (The Intercept, 7 July 2015) https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/.

- Cypriot and Bulgarian authorities provided licenses to NSO Group, whose spyware has repeatedly been linked to violations of the human rights of individuals around the world.[16]

Analysis of the final regulation

Ensuring transparency of exports: The final compromise states that the Commission shall submit a publicly available annual report to the Parliament and Council detailing per Member State the number of applications received for each type of surveillance technology, the issuing Member State, and the destination of the export.

The expanded obligations on Member States for reporting is a landmark development which will allow the public, civil society, journalists, and parliamentarians to scrutinize licensing decisions to ensure they are in accordance with law and provide an invaluable insight into the EU trade in surveillance technology.

Currently, only a handful of Member States proactively provide such information. In 2017, 11 of the 28 Member States refused to provide such information to the publication *The Correspondent* under freedom of information legislation.[17] These states included France and Italy, which are home to numerous surveillance companies.

Human rights risks being a criteria of the licensing assessment: The final agreement stipulates that Member States should "consider the risk of use in connection with internal repression or the commission of serious violations of international human rights and international humanitarian law" — a standard that has previously applied to military technology or equipment. However, the agreement does not provide criteria to determine what counts as a "serious" human rights violation. International human rights law obligates states to protect human rights. So in cases where it is clear that the exported goods will be used for human rights violations or abuses, Member States don't have discretion but are obliged to deny the export.

The Council Common Position 2008/944/CFSP is more explicit in stating that authorities shall "deny an export licence if there is a clear risk that the military technology or equipment to be exported might be used for internal repression" and "exercise special caution and vigilance in issuing licences" to countries "where serious violations of human rights have been established by the competent bodies of the United Nations, by the European Union or by the Council of Europe."[18]

---

[16] "Access Now to Bulgaria and Cyprus: don't give NSO Group license to profit from human rights violations" (Access Now, 14 May 2019) https://www.accessnow.org/access-now-to-bulgaria-and-cyprus-dont-give-nso-group-license-to-profit-from-human-rights-violations/.

[17] "How European spy technology falls into the wrong hands" (The Correspondent, 23 February 2017) https://thecorrespondent.com/6257/how-european-spy-technology-falls-into-the-wrong-hands/2168866237604-51234153.

[18] Council Common Position 2008/944/CFSP of 8 December 2008 (Official Journal of the European Union, 12 December 2008) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008E0944&from=EN.

However, as demonstrated by the continued arming of rights-abusers around the world by some Member States,[19] the existing criteria in place for military technology or equipment lack robust interpretation, implementation, and enforcement across the EU.

EU control list and "catch-all:" Currently, not all surveillance technology is subject to licensing restriction. The list of technology which is subject to licensing is currently agreed upon within international export control regimes, like the Wassenaar Arrangement, in which human rights are not key concerns and which lack transparent and consultative processes.

The new compromise will mean that if an export control authority or exporter is aware that an export may be intended "for use in connection with internal repression and/or the commission of serious violations of international human rights and international humanitarian law," and if all the other Member States agree, then that item will be subject to a licensing restriction independent of whether or not it is controlled within the international regimes.

However, while Member States can propose non-listed technology be restricted, it in effect requires unanimity and foresees no role for consulting the public or civil society organisations.

Due diligence: The new agreement includes a due diligence principle as part of the Internal Compliance Programs of larger exporters when they want to be eligible for a global export authorisation. It also mentions due diligence findings about potential risks that the export of a non-listed surveillance technology may be intended "for use in connection with internal repression and/or the commission of serious violations of international human rights and international humanitarian law."

However, this reticent formulation lacks an explicit reference to the internationally established framework of "human rights due diligence."

Neutral definition of "cyber-surveillance:" Included within the compromise is a new definition of what constitutes "cyber-surveillance" and what is therefore subject to various articles within the regulation. While it is positive that the regulation adopts a technology-neutral definition of

---

[19] "Egypt: How French Arms Were Used to Crush Dissent" (Amnesty International, September 2018) https://www.amnestyusa.org/wp-content/uploads/2018/10/How-French-Arms-were-used-to-crush-dissent-in-Egypt.pdf; "UK, France Should Join German Saudi Arms Embargo" (Human Rights Watch, 12 April 2019) https://www.hrw.org/news/2019/04/12/uk-france-should-join-german-saudi-arms-embargo; "Arms shipment to Saudi Arabia flouts multiple EU states' Arms Trade Treaty obligations' (Amnesty International, 13 May 2019) https://www.amnesty.org/en/latest/news/2019/05/arms-shipment-to-saudi-arabia-flouts-multiple-eu-states-arms-trade-treaty-obligations/; "Europe Is at War Over Arms Exports" (Foreign Policy, 18 September 2019) https://foreignpolicy.com/2019/09/18/europe-is-at-war-over-arms-exports/; "Germany violated arms export regulations for decades, study says" (Deutsche Welle, 19 July 2020) https://www.dw.com/en/germany-violated-arms-export-regulations-for-decades-study-says/a-54235639.

“cybersurveillance,” its effectiveness will depend on the Commission interpreting it broadly to cover current and new technologies that may be used to violate rights.

Recommendations

The newly adopted regulation should be considered a minimum baseline. To fulfil their international obligations to protect human rights, and under close monitoring and clear guidance by the Commission, Member States should in implementing this agreement:

- Interpret “cyber-surveillance” to include the following items which are already subject to export licensing:
    - Mobile telecommunications interception or jamming equipment;
    - Intrusion software;
    - IP network communications surveillance systems or equipment;
    - Software specially designed or modified for monitoring or analysis by law enforcement;
    - Laser acoustic detection equipment;
    - Forensic tools which extract raw data' from a computing or communications device and circumvent "authentication" or authorisation controls of the device;
    - Electronic systems or equipment, designed either for surveillance and monitoring of the electro-magnetic spectrum for military intelligence or security purpose; and
    - Unmanned Aerial Vehicles capable of conducting surveillance.

- Ensure without delay that systems specially designed to perform biometric identification of natural persons for security purposes are subject to control within the EU control list and within the Wassenaar Arrangement in a transparent and consultative process and interpret these items to constitute “cyber-surveillance.”

- Ensure detailed reports describing export license applications made to authorities concerning all dual use items are made publicly available on a regular basis, preferably monthly. These reports should at a minimum include the number of license applications per item, the exporter name, a description of the end user and destination, the value of the license, and whether the license was granted or denied and why.

- Ensure national legislation governing the assessment of export licenses takes into account relevant European human rights protections, such as the EU Charter of Fundamental Rights as well as those developed by the Court of Justice of the European Union and the European Court of Human Rights, as well as evidence by civil society and human rights experts.

- Ensure European legislation requiring corporate actors to respect human rights and implement human rights due diligence measures as prescribed by the United Nations Guiding Principles on Business and Human Rights (UNGPs). Corporate actors should be required to identify, prevent, and mitigate potential and actual adverse human rights impact of their operations and throughout their value chain. Transaction screening measures by Member States should include an assessment of the strategic nature of the items and the risks they represent for the violation of human rights. National authorities should report on the implementation activities with regard to due diligence responsibilities and obligations and encourage companies to inform the public about the scope, nature, and transferable findings of the human rights due diligence procedures they implemented. Member States and companies should also establish mechanisms to provide an effective remedy for human rights violations committed using the transferred technology.

Signatories

Access Now
Amnesty International
Committee to Protect Journalists
FIDH (International Federation for Human Rights)
Human Rights Watch
Privacy International
Reporters Without Borders (RSF)