CILD Italian Coalition for Civil Liberties and Rights

TROJAN & CO.

Surveillance technologies and export controls

CILD - ITALIAN COALITION FOR CIVIL LIBERTIES AND RIGHTS
via Monti di Pietralata, 16 – 00157 ROME - cild.eu - info@cild.eu

CILD Italian Coalition for Civil Liberties and Rights

Index

CILD - ITALIAN COALITION FOR CIVIL LIBERTIES AND RIGHTS
via Monti di Pietralata, 16 – 00157 ROME - cild.eu - info@cild.eu

Trojans – otherwise known as spyware – are powerful and invasive instruments that have been secretly used for years by many governments for the purpose of surveillance. In addition to these instruments, which hack individual devices to control their communications, the mass surveillance of digital activities is carried out by systems that monitor Internet traffic or through electronic devices like IMSI-catchers, which are used to track mobile telephones in a particular area. And if the risk of abuse is extreme in non-democratic countries, in democratic countries the status and use of similar technologies remains ambiguous. Italy and the European Union, however, are now finally trying to regulate some of these instruments.

Considered the potential for regulations within the computer and telecommunications network security context to have negative consequences upon individuals and IT security research, regulatory measures that achieve the right balance can be particularly challenging.

"Tracking and controlling exports is crucial for accountability and minimisation of the threats of uncontrolled trade in advanced surveillance capabilities used for security, law enforcement, and espionage. However, disproportionate and burdensome controls on tools that enhance privacy and security can be a threat to global stability, security and the protection of human rights" wrote nine NGOs working on digital rights in March 2017 in a letter[1] to the participants of the Wassenaar Arrangement, a multilateral export control regime with 41 participating states.

The scenario: instruments which have long been invisible

2001. The United States. News emerges that the FBI has been developing a programme that can steal the passwords used by suspected criminals to encode

[1] "Rights groups demand action on export controls", EDRi, 6 March 2017: https://edri.org/rights-groups-demand-action-export-controls/

their messages. The name of the programme is Magic Lantern. It works by sending the person under investigation what looks like an email, installs itself on their computer, and then begins to capture any passwords entered by the user. And Magic Lantern was just one of the tools used by the American agency in its IT investigations and, in particular, to get past the obstacle of cryptography, which, at the time, was primarily used in encrypted emails. "Entering a computer system is quite different from passive eavesdropping," retired UK Ministry of Defense expert Brian Gladman said to the *New Scientist*[2]. "This at least has to be highly regulated." But the regulations were late in coming.

At the technical level, instruments like Magic Lantern are considered Trojan horses. This is a kind of software that surreptitiously infects a computer and then carries out a series of actions: it can capture passwords or whatever is typed into the keyboard in general (keylogger), intercept VoIP conversations and chats, copy files, and even activate the video camera and microphone in order to carry out audio surveillance.

Already at the start of the 2000s Trojan horses had begun to be used in secret by various countries. Their use was justified by the claim that they were necessary for intercepting those kinds of communications (above all Skype) that have begun to be encrypted and thus made telephonic or online surveillance obsolete.

However, these are not the only instruments countries use to monitor digital communications. If Trojans are able to carry out in-depth surveillance but have a specific target, there are other systems used for more generalized mass surveillance. For many years now countries like the United States and Canada have been using IMSI-catchers, devices which impersonate mobile towers and are used to record, monitor, and locate all the types of mobile phones present in a particular area, in some cases even intercepting messages and voices - not to mention

[2] "FBI's "Trojan horse" program to grab passwords", W. Knight, New Scientist, 21 November 2001: https://www.newscientist.com/article/dn1589-fbis-trojan-horse-program-to-grab-passwords/

systems that monitor Internet traffic. Some of the latter, produced by European companies like Nokia Siemens Networks or Ultimaco, have been found in Tunisia, Syria, and Iran[3].

The point is that for many years we have known little to nothing about these instruments – not the people who produce them, the way they work, nor how and how often they are employed by the police and intelligence services and in which cases.

One of the key moments in Europe as regards Trojans was in October 2011, when they first began to be discussed after the Chaos Computer Club – the well-known organization of German hackers – revealed the existence of spyware in use by the federal government for investigating criminals, renaming it "Federal Trojans". Along with other various functions, Trojans were capable of recording Skype conversations and capturing screenshots. Around that same time, the Assad government in Syria was attempting to increase its mass surveillance technology capabilities for monitoring Internet traffic from various European companies like the German company AGT and the Italian company RCS Lab[4]. The French company Amesys was later accused – and the case is still open – of having sold a similar system to Gheddafi's government in Libya, reportedly used against the opposition[5].

The events of the Arab Spring brought to light western companies' sale of such technologies to authoritarian countries. The use of Trojans on the part of illiberal governments in particular, however, was highlighted by a series of reports

[3] "Monitoring Centres: Force multipliers from the surveillance industry", E. Omanovic, M. Rice, Privacy International, 29 April 2014: https://www.privacyinternational.org/node/439

[4] "European companies reportedly sold spy tools to help build Syria's surveillance system", I. Ashok, International Business Times, 13 December 2016: http://www.ibtimes.co.uk/european-companies-reportedly-sold-spy-tools-help-build-syrias-surveillance-system-1596221

[5] The Enemies of the Internet, Amesys, Reporters Without Borders (RSF): https://surveillance.rsf.org/en/amesys/

issued by Citizen Lab[6], a laboratory at the University of Toronto that studies malware (short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system[7]) and surveillance systems. Its researchers identified a series of Trojan spyware that had been produced by western companies (in particular by the Anglo-German Gamma Group/FinFisher, by the Italian Hacking Team, and the Israeli NSO Group) and found on the PCs and Smartphones of activists, journalists, and defenders of human rights in countries like Morocco, Ethiopia, Bahrain, the United Arab Emirates, Mexico, Kazakhstan, Sudan, and many others[8]. Among the first cases to appear in the press was that of the group of Moroccan journalists known as Mamfakinch who were critical of the government and thus subsequently targeted by spyware. According to Citizen Lab the software had been produced by the Italian company Hacking Team.

> In 2016 it was reported that Ahmed Mansoor, a well-known human rights defender, based in the United Arab Emirates (UAE), had been targeted for the third time by a spyware. According to research by Citizen Lab, he was previously targeted with FinFisher's FinSpy spyware in 2011, and with Hacking Team's spyware in 2012,." Once infected, Mansoor's phone would have become a digital spy in his pocket, capable of employing his iPhone's camera", wrote the researchers[9].

[6] Citizen Lab's site, research centre at the University of Toronto: https://citizenlab.org/

[7] Common examples of malware include viruses, worms, trojan horses, and spyware. Viruses, for example, can cause havoc on a computer's hard drive by deleting files or directory information. Spyware can gather data from a user's system without the user knowing it. This can include anything from the Web pages a user visits to personal information, such as credit card numbers.

[8] "Cyberwar for sale", M. Schwartz, The New York Times, 4 January 2017: https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html

[9] "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender, B. Marczak, J. Scott-Railton, Citizen Lab, 24 August 2016: https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

On March 20 2017, Mansoor was arrested in the United Arab Emirates. Amnesty International asked for his immediate release: "We believe Ahmed Mansoor was detained for the peaceful expression of his conscientiously held beliefs"[10].

According to another 2014 report by Citizen Lab, several Ethiopian journalists have also been repeatedly attacked with government trojans, some of which appeared to be Hacking Team's spyware[11].

The Bahraini government is also suspected of having infected the computers of some of the country's most prominent lawyers, activists and politicians with the malicious FinFisher spyware, according to human rights Ngo Bahrain Watch[12].

Italy, a country of surveillance

In Italy, multiple companies produce Trojans, in particular the aforementioned Hacking Team, which began working on them in the early 2000s when it first started to sell them to various police forces, public prosecutors, and Italian intelligence services before exporting and selling them to governments in dozens of other countries. Used within Italy since at least 2004, it was only in 2011 that the mainstream Italian media began to talk about such instruments following a judicial enquiry[13] into their use in the investigation of a criminal conspiracy within the public administration (the so-called P4).

[10] UAE: Surprise overnight raid leads to arrest of prominent human rights defender, Amnesty International, 20 March 2017 https://www.amnesty.org/en/latest/news/2017/03/uae-surprise-overnight-raid-leads-to-arrest-of-prominent-human-rights-defender/

[11] Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware, B. Marczak, J. Scott-Railton, S. McKune, Citizen Lab, 9 March 2015: https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/

[12] "Bahrain Government Hacked Lawyers and Activists with UK Spyware", F. Desmukh, Bahrain Watch, 7 August 2014: https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/

[13] "Un virus per pc inchioda Bisignani lo Stato diventa hacker a fin di bene", A. Sgherza, Repubblica, 22 June 2011: http://www.repubblica.it/politica/2011/06/22/news/mail_spia_hacker-18041273/

All the same, they seldom appear in the relevant court papers and are never referred to as Trojans, spyware, or malware. When they are employed in criminal investigations they are defined as information collectors, intrusive agents, and self-installed viruses. Nevertheless, their judicial status in Italy remains uncertain, and the few cases that have come to light demonstrate that their use – depending on the type of crimes – is extremely variable and discretionary.

Trojans once again appeared in the mainstream Italian press in the summer of 2015 when Hacking Team was itself hacked[14] and its documents and e-mail made available online (and then indexed by WikiLeaks). Since then, in certain settings at least, the discussion of the necessity of regulating their use has begun. Organizations like Privacy International have openly confronted the question numerous times, turning directly to the Italian authorities and demanding more stringent rules on the export of such technology[15].

Indeed, the Plenary Session of the Court of Cassation (the Supreme Judicial Court in Italy) intervened in April 2016 allowing for the use[16] of collectors in carrying out audio surveillance (among those physically present in a room) through microphones installed in electronic devices without having to indicate those places beforehand (thus allowing their use within private homes even when no crime is being committed) for investigations concerning organized crime as well as criminal conspiracies. In reality, however, the Court was simply extending the exception to the ban on surveillance in private homes (unless a crime is being committed) already in existence in the anti-mafia decree of 1991 and applying it to Trojans.

---

[14] "Con Hacking Team va su WikiLeaks un pezzo di Stato italiano", C. Frediani, La Stampa, 10 July 2015: http://www.lastampa.it/2015/07/10/tecnologia/con-hacking-team-va-su-wikileaks-un-pezzo-di-stato-italiano-mY6laMRZb1g7zJlSx4kOll/pagina.html

[15] "Con Hacking Team va su WikiLeaks un pezzo di Stato italiano", ibid., http://www.lastampa.it/2015/07/10/tecnologia/con-hacking-team-va-su-wikileaks-un-pezzo-di-stato-italiano-mY6laMRZb1g7zJlSx4kOll/pagina.html

[16] "Corte di Cassazione, Sezioni Unite, Sentenza 1 July 2016, n.26889 Ricognizione, Nel Diritto: http://www.neldiritto.it/appgiurisprudenza.asp?id=13067

Nevertheless, even if its decision only referred to one of the many functions of Trojans by some this was seen as a partial green light.

The European panorama

The European Union only began paying attention for two primary reasons: after a series of international reports – from Citizen Lab's first investigations[17] which came back to light in 2012[18] to the papers released by Fidh.org[19], a federation of human rights NGOs – highlighted certain European producers of intrusive surveillance technology and its sale to authoritarian countries; and when such *made in Europe* malware was found on the devices of journalists, dissidents, and lawyers in countries where the violation of human rights were very frequent – as, for example, in Bahrain[20] or in the United Arab Emirates where in 2015 the human rights activist Ahmed Mansoor was bombarded[21] for the third time with spyware (this last time apparently with Israeli-created malware).

Since 2014 the EU has tried to impede the uncontrolled sale of surveillance technology, thanks in part to pressure[22] from CAUSE: the Coalition Against Unlawful Surveillance Exports, a coalition of NGOs like Privacy International,

---

17 "For Their Eyes Only: The Commercialization of Digital Spying", M. Marquis-Boire, B. Marczak, C. Guarnieri, J. Scott-Railton, Citizen Lab, 30 April 2013: https://citizenlab.org/2013/04/for-their-eyes-only-2/

18 "From Bahrain with Love: FinFisher's Spy Kit Exposed?", M. Marquis-Boire, Citizen Lab, July 2012: https://citizenlab.org/wp-content/uploads/2012/08/09-2012-frombahrainwithlove.pdf

19 "Surveillance technologies "made in Europe": regulation needed to prevent human rights abuses", C.Perarnaud, A. Klocke, G. Paul, International Federation for Human Rights, December 2014: https://www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe.pdf

20 "Bahrain Government Hacked Lawyers and Activists with UK Spyware", ibid.

21 "iPhone vulnerabile a spyware, le falle scoperte da attivista sotto attacco", C. Frediani, La Stampa, 26 August 2016: http://www.lastampa.it/2016/08/26/tecnologia/news/iphone-vulnerabile-a-spyware-le-falle-scoperte-da-attivista-sotto-attacco-5zVY7rhgLFDLUVnwSUtcxH/pagina.html

22 "A critical opportunity: bringing surveillance technologies within the EU Dual-Use Regulation", Steering Committee of the Coalition Against Unlawful Surveillance Exports (CAUSE), June 2015: https://www.privacyinternational.org/sites/default/files/CAUSE_8.pdf

Amnesty International, Human Rights Watch, Digitale Gesellschaft, Open Technology Institute and Reporters without Borders[23].

Up until now some of these technologies have not been considered dual-use products, which means that they can be used both in civilian and military environments (and which means that, as such, they should be subjected to stricter control). These products can be chemical substances, toxins, equipment or components used in the manufacturing of weapons, and some information technology. In particular, EU council regulation N. 428/2009[24] on the control of dual-use items (EU Regulation (EC) N°428/2009) allowed Member States to implement them at a national level, and provided them with the consequent legal framework. In Article 8 of the same regulation, the Member States were allowed, for example, to request export authorization for those dual-use products not included on the list for reasons of public security and human rights. These "catch-all" clauses have only rarely been used by Member States, however, and their implementation has been considered too discretional.

Therefore on October 22, 2014, the European Commission announced an update of the list of dual-use goods in line with other voluntary international accords on the regulation of arms exports and dual-use technologies (the Wassenaar Arrangement) and to reflect the growing preoccupation with the use of surveillance technologies and other cyber instruments that can violate human rights. The adapted list introduces controls for new categories like intrusive software (spyware) and IP surveillance devices that allow for the monitoring of Internet traffic. These regulations went into effect at the end of that year.

[23] "Surveillance technologies "made in Europe": regulation needed to prevent human rights abuses", ibid., https://www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe.pdf

[24] "REGOLAMENTO (CE) N. 428/2009 del Consiglio del 5 May 2009 che istituisce un regime comunitario di controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di prodotti a duplice uso", 5 May 2009: http://www.sviluppoeconomico.gov.it/images/stories/commercio_internazionale/embarghi_dualuse/reg428_09.pdf

It is important to state that the Wassenaar Arrangement[25] control does not target the Trojan component, but rather the command and control infrastructure used to generate, install and instruct the Trojan – i.e., the software installed on a government controlled server to deliver the Trojan to a target address.

Even so, this modification does not seem to have impeded the export of these technologies to non-democratic states with grave issues of human rights violations. An international investigation – Security for Sale[26] – conducted by a network of European journalists and published in 2017 demonstrated that in the last three years the Member States of the EU have permitted the export of cyber-surveillance technology at least 317 times and only denied them 14 times. Furthermore, almost a third of the permits were for countries which had been defined as "not free" by the organization Freedom House[27], which monitors human rights throughout the world, while 52 per cent of permits were directed to countries, like Turkey, classified by the same organization as "partially free". These numbers, however, are incomplete. Of the 28 Member States, 11 refused to give information on their exports, France and Italy among them. As Security for Sale notes, the two countries are "both seats of some of the major global business players of surveillance technologies."

The European Commission has realized the necessity of making the rules more clear, more binding, and more uniform; and, as we shall see, it has come up with a new proposal that goes in just such a direction, increasing the number of technologies to be controlled as well as strengthening the emphasis on the necessity of considering human rights in the granting of permits.

---

[25] The Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies: http://www.wassenaar.org/

[26] "Security for Sale The price we pay to protect Europeans", The Correspondent, 7 March 2017: https://thecorrespondent.com/10221/security-for-sale-the-price-we-pay-to-protect-europeans/497732037-a3c8cc9e

[27] "Populists and Autocrats: The Dual Threat to Global Democracy", Freedom House, 2017: https://freedomhouse.org/report/freedom-world/freedom-world-2017

Focus: Italian exports

Within the global surveillance industry, Italy has carved out one of the top spaces after the United States, Great Britain, France, Germany, and Israel. Indeed, according to Privacy International[28], around 18 Italian companies are active in the sector and over the last few years Italy, in addition to being a constant in the defence industry, has developed a strong surveillance industry – in part as an extension of a system already in place, in part in the fight against crime.

The two Italian companies that have most often fallen under international scrutiny thanks to their exports are, once again, Hacking Team and Area. For years Hacking Team, the number one Italian producer of spyware, has exported its products undisturbed, including to countries like Russia[29] and Sudan[30]. At the beginning of 2015, when even Trojans appeared on the European list of dual-use products requiring authorization for their export, Hacking Team had already received such authorization[31] from the Ministry of Economic Development (MISE), in effect, a clear go-ahead. That permit, however, was rescinded[32] in April 2016, possibly as a delayed reaction to the Citizen Lab report or, what's more likely, to media attention concerning the murder of the Italian researcher Giulio Regeni in Egypt. Since then, the company has had to obtain specific, individual authorization for all exports to countries outside of Europe.

---

28 "iPhone vulnerabile a spyware, le falle scoperte da attivista sotto attacco", ibid.: http://www.lastampa.it/2016/08/26/tecnologia/news/iphone-vulnerabile-a-spyware-le-falle-scoperte-da-attivista-sotto-attacco-5zVY7rhgLFDLUVnwSUtcxH/pagina.html

29 "Intelligence o panini? La doppia vita di Hacking Team", C. Frediani, La Stampa, 14 July 2015: http://www.lastampa.it/2015/07/14/tecnologia/intelligence-o-panini-la-doppia-vita-di-hacking-team-AuCZyCJquh8XyS68bhaYaP/pagina.html

30 "Così il Sudan ha messo in crisi Hacking Team", C. Frediani, La Stampa, 9 July 2015: http://www.lastampa.it/2015/07/09/tecnologia/cos-il-sudan-ha-messo-in-crisi-hacking-team-6oxJBVvCJUvCshTr1uSqWK/pagina.html

31 "Dual use - Prodotti tecnologici a duplice uso", Ministero dello Sviluppo Economico (last accessed: 18 March 2017): http://www.sviluppoeconomico.gov.it/index.php/it/component/content/article?id=2022475

32 "Hacking Team, revocata l'autorizzazione globale all'export del software spia: stop anche per l'Egitto dopo il caso Regeni", A. Pitoni, Il Fatto Quotidiano, 6 April 2016: http://www.ilfattoquotidiano.it/2016/04/06/hacking-team-revocata-lautorizzazione-globale-allexport-del-software-spia-stop-anche-per-legitto-dopo-il-caso-regeni/2610721/

The national authorities' regulatory uncertainty, however, was also exposed by another event. In June 2016 the Ministry of Economic Development gave an Italian company, Area S.p.A., the specific authorization to export surveillance technology to Egypt. The end client was the Technical Research Department (TRD) of the National Defence Council, an arm of the Egyptian intelligence services which, according to an earlier report from Privacy International, completely lacked any kind of oversight and for years had been acquiring various surveillance technologies from European companies. However, in January 2017, after the publication of a letter to the MISE written by CILD together with Privacy International and the Hermes Center for Transparency and Digital Human Rights in which they sought explanation for the authorization given to Area, the Ministry responded with a note[33] stating that the process of re-evaluation of said authorization had been begun the previous July and that its definitive revocation had been scheduled for the next meeting of the special Committee. In addition, in December 2016 Area had been searched and served with a preventive seizure[34] order of 7.7 million euros in the context of an investigation concerning the alleged violation of the laws regarding the export of dual-use technologies to Syria between 2010 and 2011. The authorization is still suspended with a final decision scheduled on the following June 27th[35].

In April 2017, Al-Jazeera released and aired "Spy Merchants"[36], a documentary that included undercover footage, showing a number of Italian and international surveillance company representatives willing to export surveillance equipment

[33] "Il MISE risponde alla nostra lettera: la licenza di Area spa sarà revocata", CILD, 24 January 2017: https://cild.eu/blog/2017/04/11/sorveglianza-e-aziende-italiane-le-esportazioni-verso-regimi-repressivi-continuano-la-nostra-lettera-al-mise/

[34] "Esportava un sistema di monitoraggio internet ai servizi siriani": come è nata l'ipotesi di reato che ha travolto Area", C. Frediani, La Stampa, 5 December 2016: http://www.lastampa.it/2016/12/05/italia/cronache/esportava-un-sistema-di-monitoraggio-internet-ai-servizi-siriani-come-nata-lipotesi-di-reato-che-ha-travolto-area-qVSJ1zMIDGoODZfH4jSRMK/pagina.html

[35] Risposta scritta pubblicata Mercoledì 12 aprile 2017 nell'allegato al bollettino in Commissione X (Attività produttive) 5-11055, 12 April 2017: http://aic.camera.it/aic/scheda.html?numero=5/11055&ramo=CAMERA&leg=17

[36] "Spy Merchants", Al Jazeera, 10 April 2017: https://www.aljazeera.com/spymerchants

with little regard to human rights. CILD, Privacy International and the Hermes Center for Transparency and Digital Human Rights wrote again to the Ministry asking to release information related to the license and advocating for more transparency and accountability for the industry[37].
As of today, in addition to Syria, the export of dual-use technologies from Europe to the following countries has been restricted[38]: Iran, North Korea, Russia, Ukraine, and Crimea.

Towards a new European regulatory framework?

As mentioned above, at the end of 2016 the European Commission proposed[39] reinforcing controls on the exportation of dual-use goods.

The Commission, the European Parliament and the Council have previously stated that modernisation of the system was needed in order to keep up with new threats and rapid technological changes, to reduce distortions and to create a genuine common market for dual-use items. A 2014 joint statement[40] recognised that controls were needed on the export of certain information and communication technologies (ICT) that can be used in connection with human rights violations and to undermine the EU's security.

In particular, controls refer to the dimension of "human security" in evaluating authorizations in order to avoid the violation of rights through cyber surveillance

[37] Esportazioni di cybersorveglianza, l'Italia torna nel mirino, C. Frediani, La Stampa, 11 April 2017: http://www.lastampa.it/2017/04/11/esteri/esportazioni-di-cybersorveglianza-italia-torna-nel-mirino-OVCGrUFyFqxyAtE5pQxDaJ/pagina.html

[38] Dual use - Prodotti tecnologici a duplice uso", Ministero dello Sviluppo Economico (last accessed: 18 March 2017): http://www.sviluppoeconomico.gov.it/index.php/it/component/content/article?id=2022475

[39] "Commission proposes to modernise and strengthen controls on exports of dual-use items", Commissione Europea, 28 settembre 2016: http://europa.eu/rapid/press-release_IP-16-3190_en.htm

[40] Regulation (EU) No 599/2014 of the European Parliament and of 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 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0599

technologies. The proposal also includes the harmonization of the rules and procedures adopted by the various Member States.

The list of technologies to be covered by the new regulation include:

- mobile telecommunications interception equipment;
- intrusion software (Trojans);
- monitoring centres;
- lawful interception systems and data-retention systems;
- digital forensics.

The first three technologies had already been included on the list concerning the control of dual-use technologies in the Wassenaar Agreement and in December 2014 were added to the EU list.

The current proposa[41]l is being considered[42] as we speak: it began to be discussed in the European Parliament on February 28, 2017. As stated in the briefing: "The proposed regulation recasts the regulation in force since 2009. Among other elements, the proposal introduces a controversial new 'human security' dimension to export controls, to prevent the abuse of certain cyber-surveillance technologies by regimes with a questionable human rights record.

Stakeholders are divided over the incorporation of human rights considerations, with the technology industry particularly concerned that it might lose out to non-European competitors."

---

[41] "Review of dual-use export controls - briefing", European Parliament, 30 January 2017: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf

[42] "Review Of Dual-Use Export Controls [EU Legislation In Progress]", B. Immnkamp, European Parliamentary Research Service Blog, 11 January 2017: https://epthinktank.eu/2017/01/11/review-of-dual-use-export-controls-eu-legislation-in-progress/

[43] "Rights Organisations Urge Export Control Body to Change Control List", Privacy International, 6 March 2017: https://medium.com/privacy-international/rights-organisations-urge-export-control-body-to-change-control-list-997c209c6aa4

In March 2017, rights organisations from around the world sent a joint letter[43] to all participating states of the Wassenaar Arrangement urging its participants to update rules to protect human rights and security research, raising concerns about its broadness, and its potential impact on the ability for the information security community to conduct research.

This report was finalized in April 2017

TROJAN & CO.

Surveillance technologies
and export controls

PRODUCED BY

CILD

CILD - ITALIAN COALITION FOR CIVIL LIBERTIES AND RIGHTS
via Monti di Pietralata, 16 – 00157 ROME - cild.eu - info@cild.eu