Mass Surveillance Technology: Trading Trojan Horses?

LIA CAPONETTI[1]

Abstract

This paper challenges the effectiveness and necessity of "mass surveillance technology"(MST) on two dimensions: (a) states' internal use of MST and the subsequent issue of violation of fundamental freedoms, and (b) surveillance technology export control, especially to third countries likely to use such technology to violate human rights. Following the Snowden Datagate scandal, many States undertook inquiries and adopted measures that, in some cases, were meant to regulate the use of mass surveillance technology. The paper will: a) assess and evaluate current regulations on mass surveillance technology and its place in democratic societies, including what is at stake in terms of technology, threats, reactions to threats, and geographic extension, b) the risks linked to the use of MST on the national level by questioning the validity of counter-terrorism measures as a justification for MST use c) analyze international trade control regimes and legislation to highlighting their inadequacy in the face of the threats posed by MST, and d) map the evolution of the EU dual-use trade control system towards a human security approach with regard to human rights protection, in order to assess the capability of the system to avoid the misuse of MST.

Keywords

Mass surveillance technology, trade controls, cyber-security, human security, human rights, EU Dual-use Regulation

Introduction

> *Whether we like it or not, the international norms of tomorrow are being constructed today, right now, by the work of bodies like this Committee. If liberal States decide that the convenience of spies is more valuable than the rights of their citizens, the inevitable result will be States that are both less liberal and less safe.*

With these words, Edward Snowden concluded his testimony to the European Parliament (EP) as part of the EP's inquiry on Electronic Mass Surveillance of EU Citizens.[2] Since Snowden's disclosures on

[1] Lia Caponetti is a junior researcher and assistant at the European Studies Unit (ESU) of the University of Liège (Belgium), where she has worked since October 2013.

[2] Edward Snowden is a former contractor for the CIA. He left the US in late May 2013 after leaking to the media details of extensive Internet and phone surveillance by American intelligence. Mr Snowden, who has been granted temporary asylum in Russia, faces espionage charges. The scandal broke in early June 2013, when The Guardian newspaper reported that the US National Security Agency (NSA) was collecting the telephone records of tens of millions of Americans. The paper published the secret court order directing telecommunications company Verizon to hand over all of its telephone data to the NSA on an "ongoing daily basis." That report was followed by revelations in both The Washington Post and The Guardian that the NSA tapped directly into the servers of nine internet firms including Facebook, Google, Microsoft and Yahoo to track online communication in a surveillance programme known as Prism. See "Edward Snowden: Leaks that Exposed US Spy Programme,"

controversial mass surveillance programmes by intelligence and national security agencies, MST has been in the spotlight of public debate and political inquiries.[3,4]

The EP was particularly active on this front, conducting a series of studies and inquiries. For instance, through the Committee on Civil Liberties, Justice and Home Affairs (LIBE) in collaboration with national Parliaments and the EU-US expert group, the EP published a report and a resolution on 21 February 2014 and 12 March 2014, respectively.[5,6,7] A study was also conducted via the Directorate General for Internal Policies entitled National Programs of Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law, examining mass surveillance practices in five EU countries: France, Germany, Sweden, Netherlands, and the United Kingdom. The study found that a network called "Five Eyes," dating back to 1946, gathered the intelligence services of five countries (US, UK, Canada, Australia and New Zealand) and cooperated on signals intelligence and other activities extended over time (Echelon and now Fornsat).[8] Finally, the report 'Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries' (2014/2232(INI)) was published, on 3 June 2015, by Member of European Parliament (MEP) Marietje Schaake.[9] The report was followed by the adoption of a resolution, published on 8 September 2015.[10]

Three international developments took place in this regard. The first was the publication by the UN Special Rapporteur of a report, 'Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism,' denouncing the situation regarding mass surveillance and the lack of effective judicial control.[11] The second was another report, adopted by the Council of Europe Committee on Legal Affairs and Human Rights of the Parliamentary Assembly, on mass surveillance adopted unanimously on 26 January 2015.[12] The third was the implementation of export controls related to some "Intrusion Software" and "IP Network Surveillance Systems" within the Wassenaar Arrangement (WA) and within the EU via the entry into force, on 22 October 2014, of the Commission Delegated Regulation (EU) No 1382/2014

BBC News, January 14, 2014.

[3] Edward Snowden, "Edward Snowden' Testimony," European Parliament, March 7, 2014, <http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf>.

[4] UK intelligence and security Committee inquiry, the Dutch CTIVD inquiry, the Brazilian Senate investigation fóf NSA spying in Brazil, the European Parliament Civil Liberties Committee investigation on electronic surveillance, the Australian Senate inquiry into revision of the Telecommunications Act, the German Bundestag launch of the NSA Investigation Committee, the Council of Europe reports on whistleblowing and mass surveillance.

[5] The LIBE Committee was instructed to conduct the inquiry in European Parliament resolution of 4 July 2013, see European Parliament, "The US National Security Agency Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Privacy," 2013/2682(RSP), July 4, 2013, < http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0322+0+DOC+XML+V0//ENZ.

[6] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur Claude Moraes, "Draft Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs," 2013/2188(INI), February 21, 2014, < http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-526.085%2B02%2BDOC%2BPDF%2BV0%2F%2FEN>.

[7] European Parliament resolution of 12 March 2014 on "The US NSA surveillance programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs," 2013/2188(INI), July 4, 2013.

[8] For more information on surveillance, including Echelon/Fornsat, see European Parliament, "Interception Capabilities, " 2014, <http://www.europarl.europa.eu/document/activities/cont/201309/20130916ATT71388/20130916ATT71388EN.pdf.>.

[9] European Parliament, Committee on Foreign Affairs, Rapporteur Marietje Schaake, "Report on Human Rights and Technology: the Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries," 2014/2232(INI), June 3, 2015.

[10] European Parliament resolution of 8 September 2015, "Human Rights and Technology: the Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries," 2014/2232(INI), September 8, 2015.

[11] United Nations Office of the High Commissioner for Human Rights, Report on Promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/397, September 23, 2014.

[12] Parliamentary Assembly, "Report on Mass Surveillance," Doc. 13734, March 18, 2015.

updating Annex I.[13,14]

The so-called "Snowden Datagate" brought into the spotlight not only intelligence and national security agencies but also suppliers of the "spyware industry." Scandals involving European industries providing mass surveillance technology to authoritarian States drew attention to companies such as the Italian Hacking Team or the British-German Gamma Group, also know as FinFisher. The Italian company, for example, has been accused by MEP Schaake of exporting spy tools to repressive regimes such as Russia and Sudan and violating European sanctions, in some cases. The MEP also blamed the Italian competent authority for having issued a global authorisation to Hacking Team, allowing the company to export its products freely in all countries of the WA.[15]

As new threats emerge and technology continues rapid development, States' capacity to regulate cyberspace, as well as their security approach, is questioned vis-à-vis the growing violation of citizens' privacy and, in some States, of human rights. On the one hand, some trade control regimes try to keep pace and evolve to control technologies that could violate human rights, shifting their paradigm from a purely strategic to a more human security approach. On the other hand, the fight against terrorism seems to be, still, a sound reason to scratch ground to fundamental freedoms.

Through the analysis of official documents, reports and legislation on the topic, this paper will assess the situation on the control and use of mass surveillance technology the national and international level. The paper will argue that because of the risks related to the use of MST on states' domestic systems (such as the violation of the right to privacy) and the inadequacy of international trade controls regimes and legislation to prevent these risks, MST not only is ineffective in its declared security purpose, but it is also dangerous for the very foundations of democratic societies. The European Union dual-use trade control system will serve as an example to show incompatibilities between fundamental freedoms and MST. An analysis of the evolution of the EU system towards a "human security" approach when dealing with trade controls will show loopholes and limits of the system.

Targeted Surveillance vs. Mass Surveillance: National-Level Mass Surveillance Technology Risks

This section deals with the dangers posed by mass surveillance technology on the national level. To understand the dangers of this technology, it is first important to understand the difference between mass surveillance and targeted surveillance. While the latter is a valuable instrument for countering terrorism and preventing other delinquent acts, the former is a violation of fundamental freedoms, especially the right to privacy and to data protection. While targeted surveillance is subject to prior judicial authorisation and respects the criteria of proportionality and legal necessity, mass surveillance represents a permanent delegation to dodge the law.

The issue is being particularly debated at the UN and European level under the lead of the European Parliament. The UN report 'Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism' makes the distinction between targeted surveillance and mass surveillance, identifying the former as a valuable means to counter terrorism. In fact, targeted surveillance of suspected individuals and organizations allows intelligence and law enforcement agencies "to intercept and monitor

[13] It seems that the WA' s decision to implement export controls on some "Intrusion Software" and "IP Network Surveillance Systems" came after an open letter sent by a coalition of human rights organisations (led by the Coalition Against Unlawful Surveillance Exports - CAUSE) to the WA, in order to push the international regime to implement such controls.

[14] Wassenaar Arrangement, "Public Statement 2013 Plenary Meeting of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies," Vienna, December 4, 2013, <www.wassenaar.org>.

[15] Marietje Schaake, "Hacking Team Company at Receiving End of Hacks," Marietje Schaake's Blog, posted on July 7, 2015, <www.marietjeschaake.eu>.

calls made on a landline or mobile telephone, enabling an individual's location to be determined, his or her movements to be tracked through cell site analysis and his or her text messages to be read and recorded. Targeted surveillance also enables (…) to monitor the online activity of particular individuals, to penetrate databases and cloud facilities, and to capture the information stored on them."[16]

The main feature of targeted surveillance is that it depends upon the existence of prior suspicion of the targeted individual/organisation. From a procedural and legal point of view, it also means that a prior authorisation for surveillance is required, whether judicial or executive, to assess the legality and proportionality of surveillance measures by reference to the facts of the specific case. In other words, targeted surveillance is a preventive security measure, applied by intelligence and enforcement agencies following a judicial or executive authorisation, which is issued on a case-by-case basis assessing the necessity and the proportionality of the measures to apply.

Several States secured bulk access to communications and content data without prior suspicion. As explained in the UN report:

> *Relevant authorities in these States are now able to apply automated "data mining" algorithms to dragnet a potentially limitless universe of communications traffic. By placing taps on fibre-optic cables through which the majority of digital communications travel, relevant States have thus been able to conduct mass surveillance of communications content and metadata, providing intelligence and law enforcement agencies with the opportunity to monitor and record not only their own citizens' communications, but also the communications of individuals located in other States.*[17]

The study on mass surveillance realised in December 2014 by the EP Research Service Science and Technology Options Assessment (STOA) also makes the distinction between "mass unwarranted and indiscriminate interception" and "targeted lawful interception of Internet and telephony data for the purpose of law enforcement and crime investigation."[18] While this latter is considered a necessary and legitimate instrument, the former is seen as a threat to civil liberties such as the right to freedom of opinion and expression.

The STOA study also explains the difference between communication data and meta-data and focuses on practices of interception and analysis of end-user meta-data. This latter is defined as data that is produced when electronic communication channels are used and provides information about the time, origin, destination, location, duration and frequency of the communications carried out. However, meta-data does not contain the content of communications.[19] This distinction is particularly important since while meta-data is considered personal data under UE legislation, it is not the case for all foreign legislation and notably, it is not the case for US legislation.

Both the UN report and the STOA study explain how telecommunications and Internet service providers cooperate, although not always in a "spontaneous" way, regarding the collection of data and meta-data for mass surveillance purposes. For example, the EP Working Document on the Follow-up of the LIBE Inquiry

---

[16] United Nations, "Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism," A/69/397, September 23, 2014, < https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf>, pp. 3-4.

[17] Ibid, p. 4.

[18] European Parliament, European Parliamentary Research Service Science and Technology Options Assessment (STOA), "Mass Surveillance: What are the Risks for the Citizens and the Opportunities for the European Information Society? What are the Possible Mitigation Strategies?," Study IP/G/STOA/FWC-2013-1/LOT9/C5/SC1, December 2014.

[19] Another distinction, within meta-data, is between meta-data of the communication (e.g. sender, receiver, communication duration, communication channel, etc.) and meta-data on the content (e.g. read/write/modify, attributes of the file, author of the document, GPS location of a picture, etc.) and within communication meta-data, two further subcategories are Telephony meta-data and Internet meta-data (also-called Internet Protocol (IP) meta-data).

on Electronic Mass Surveillance of EU Citizens reports that three of the major phone networks in the UK including EE, Vodafone and Three, gave police mobile call records without requiring staff to initiate a review of all police information requests.[20] In addition, in the UK telecommunications company Cable and Wireless was bought by Vodafone in July 2012, provided UK GCHQ with access to Internet traffic.[21] The company was part of a programme called "Mastering the Internet" operated under the pseudonym "Gerontic."[22]

It is worthwhile noticing that States' capacity to collect citizens' data is reinforced by mandatory data retention laws that require telecommunications and Internet service providers to preserve communications data for inspection analysis. However, as reported by the STOA study, methodologies to obtain this kind of data from telecommunications and Internet service providers can also be less "orthodox" than on the basis of a lawful request. Threats of fines or "undeclared" capabilities to break system protections and to infiltrate systems and networks by applying advanced hard and software technology seem to be additional ways to access citizens' data. For example, in September 2013, Belgacom denounced to the criminal judicial authorities a hacking incident affecting the company. Press coverage and IT security company Symantec reported that Belgacom had been the victim of a complex malware called REGIN that allegedly originated in US or UK intelligence agencies.[23]

Going back to the criteria for lawful targeted surveillance, the UN report points out three main criteria to assess whether surveillance is lawful or not. The starting point for the assessment is Article 17 of the International Covenant on Civil and Political Rights, considered the most important legally binding treaty provision guaranteeing the right to privacy at the universal level.[24] The article provides:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation;

2. Everyone has the right to the protection of the law against such interference or attacks.[25]

It is acknowledged that, although the article does not contain a clause specifying the conditions in which such a right could be limited, the UN report delineates three conditions allowing for the restriction of the right to privacy:[26]

1. Restrictions/interference/surveillance measures are authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant;

2. Such measures pursue a legitimate aim;

3. They meet the test of necessity and proportionality.

---

[20] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Claude Moraes, "Working Document on the Follow-up of the LIBE Inquiry on Electronic Mass Surveillance of EU Citizens," January 19, 2015.

[21] GCHQ, which stands for Government Communications Headquarters, is UK' security and intelligence organisation (the equivalent of US' NSA).

[22] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Claude Moraes, "Working Document on the Follow-up of the LIBE Inquiry on Electronic Mass Surveillance of EU Citizens," January 19, 2015.

[23] Ibid.

[24] All EU Member States are States Parties to the Covenant, as well as the United States (which, however, are not State Party as regard to the Optional Protocol to the International Covenant on Civil and Political Rights of 1976), New Zealand, Australia and Canada. To check the status of a specific State, use the following link: <http://indicators.ohchr.org>.

[25] United Nations, International Covenant on Civil and Political Rights, General Assembly resolution 2200A, March 23, 1976.

[26] United Nations, "Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism," A/69/397, September 23, 2014, < https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf>, p.12.

Still, at the supra-national level, EU Member States are even more engaged to the right to privacy and protection of personal data by the Charter of Fundamental Rights (CFR) of the European Union, annexed to the Lisbon treaty and which acquired legally binding status on 1 December 2009. Article 7 of the Charter states that, "everyone has the right to respect for his or her private and family life, home and communications."[27]

Article 8 of the Charter lays down provisions for the protection of personal data.[28] However, the rights may be restricted, as established by Article 52(1), on the basis of some preconditions. Notably, the restrictions must be done lawfully, respecting the principle of proportionality and necessity as well as genuinely meeting objectives of the general interest recognised by the Union.[29]

These conditions/criteria listed in the UN report and established in the CFR of the EU are not met by mass surveillance programmes, first of all because of the lack of proportionality and of a case-by-case analysis. The use of bulk access to all digital communications traffic eliminates *a priori* any possibility of individualized proportionality analysis. Since there is no target-specific justification for mass surveillance, states seek to justify the general practice of bulk access and "data-mining" to and of digital communications, shifting, in this way, the proportionality analysis "from the micro level (assessing the justification for invading a particular individual's or organisation's privacy) to the macro level (assessing the justification for adopting a system that involves wholesale interference with the individual and collective privacy rights of all Internet users)."[30]

As for the necessity of mass surveillance programmes, states engaged in the activity have so far failed to provide a detailed and evidence-based public justification for its necessity and almost no state has enacted explicit domestic legislation to authorise its use. The threat of terrorism can provide a justification for mass surveillance but evidence should be shown as to the real utility of such technologies in countering it.[31]

The final UN Report, led by UN Rapporteur Claude Moraes on the EU inquiry conducted by the LIBE Committee on the US NSA surveillance programme, arrives to the same conclusion when, in the main findings, it notes that the claim that mass surveillance programmes are necessary to combat terrorism cannot be a justification for untargeted, secret or even illegal mass surveillance programmes because they are incompatible with the principles of necessity and proportionality in a democratic society. Finally, the report considers that "data collection of such magnitude leaves considerable doubts as to whether these actions are guided only by the fight against terrorism, since it involves the collection of all possible data of all citizens."[32]

On the issue of proportionality, the European Court of Justice, in the judgement of 8 April 2014, in joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, declared the EU Data Retention Directive 2006/24/EC to be invalid.[33] In fact, the CJEU is of the opinion that, by adopting this Directive, the EU legislature exceeded the limits imposed by compliance with the principle of proportionality. The

---

[27] European Union, Charter of Fundamental Rights of the European Union, Official Journal of the European Union (C 364/1), December 18, 2000.

[28] Ibid.

[29] Ibid.

[30] United Nations, "Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism," A/69/397, September 23, 2014, < https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf>, p.5.

[31] [31] Edward Snowden, "Edward Snowden' Testimony," European Parliament, March 7, 2014, <http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf>, pp. 1-2.

[32] European Parliament, "Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs," 2013/2188(INI), February 21, 2014, pp. 20-21.

[33] European Court of Justice, "Judgement of the Court (Grand Chamber) of 8 April 2014, in Joint Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others," Official Journal of the European Union, (C 175/6), June 10, 2014.

objective of the Directive was to harmonise Member States' provisions concerning the retention of certain data generated or processed by providers of publicly available electronic communications services or of public communications networks. The general aim of the Directive, therefore, was to make this data available for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as, in particular, organised crime and terrorism. With this aim, the Directive obliged providers to retain traffic and location data as well as related data necessary to identify subscribers or users, although it did not permit the retention of the content of the communication or of information consulted. Despite this exclusion, the Court judged that the retention of the data allowed by the Directive was more than sufficient to provide very precise information on the private lives of the persons whose data was retained. By consequence, the Directive interfered in a serious manner with fundamental rights to respect for private life and to protection of personal data, especially since data could be used without the subscriber or user being informed. The Court considered that, although the retention of data required by the Directive could be appropriate to attain the objective of the Directive, namely the fight against serious crime and, ultimately, public security, the wide-ranging and serious interference of the Directive with fundamental rights at stake is not sufficiently circumscribed to ensure that the interference is actually limited to what is strictly necessary. In fact, the Directive covers in an overly generalised way all individuals, all means of electronic communication, and all traffic data without any differentiation, limitation or exception. Furthermore, it does not lay down substantive and procedural conditions under which the competent national authorities may have access to the data and use them and, above all, the access to the data is not subject to a prior review by a court or an independent administrative body. In other words, the Court identified a risk of abuse, aggravated by the vague definition of the data retention period identified in a timeframe between six months and twenty-four months, without any further specifications.

On the issue of surveillance and, in particular mass surveillance, some states' legislation displays several loopholes and, above all, lack of transparency. While several states are filling these loopholes by strengthening individuals' rights in cyber-space, other states are going in the opposite direction by "legalising" practices of mass surveillance. The UK and the Netherlands are examples of this latter category of states. On 18 July 2014, the UK Parliament adopted the Data Retention and Investigatory Powers Act which expands surveillance powers by empowering the UK Secretary of State for the Home Department to issue interception warrants for communications content that is stored outside of UK territorial jurisdiction and gives UK authorities broad powers to obtain, access and store communications meta-data. Legislative proposals were also made in the Netherlands to introduce an amendment to the Dutch Intelligence and Security Act 2002 allowing for intelligence services to also intercept cable-bound communications.[34]

Mass Surveillance Technologies and Suppliers: Who Exports What and Why?

This section explores the international dimension of the risks linked to the export of mass surveillance technology, in particular in the field of human rights protection. It is useful first to identify the scope of this kind of technology in terms of the object (what it is), in terms of subject (who provides it) and in terms of location (where is it/where is it exported).

Once identified, the "traffic" of mass surveillance technology in international trade and the relationships between suppliers and end-users will be considered with a particular focus on the relation between suppliers and national authorities as end-users. The objective is to "raise a red flag" on the conflict of interest that exists between the State as legislator of trade controls and guarantor of fundamental freedoms, and its role as end-user of mass surveillance technology. The risk of such a close relationship, in fact, could result in "permissive" legislation or policy implementation and/or in a degree of "blind" policy implementation leaving legislative loopholes in the system.

Mass surveillance technology is part of the wider ICT sector (information and telecommunication

[34] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Claude Moraes, "Working Document on the Follow-up of the LIBE Inquiry on Electronic Mass Surveillance of EU Citizens," January 19, 2015.

technologies). The ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights divides the ICT sector in five main segments (for more technical details, please see the table in Annex I):[35]

- Telecommunications services;
- Web-based (and cloud-based) services/platforms;
- Manufacture of consumer and business end-user devices ("device manufacturer");
- Manufacture of telecommunications components, device components and network equipment ("component manufacturers");
- Software.

The Wall Street Journal (WSJ) reported in 2011 that "a retail market for surveillance tools has sprung up from 'nearly zero' in 2001 to about $5 billion a year."[36] More precisely, the WSJ reported that "a new global market for the off-the-shelf surveillance technology has arisen in the decade since the terrorist attacks of September 11, 2001," linking the "war on terror" and the spread of surveillance technology.[37] According to the paper *Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age*, the 9/11 terrorist attacks, as well as other terrorist attacks in Bali, Madrid, London and Mumbai, were perceived as intelligence failures, and generated the "need" for better intelligence-gathering capabilities.[38]

In addition, the market for surveillance technology grew due to the existence of legislative and regulatory loopholes allowing intelligence and law enforcement agencies to profit from systemic gaps to use data not subject to regulation. The increasing dependency of governments on the private sector, which seems more capable of keeping the pace with technological changes and demands, also contributes to to growth in the sector.

However, surveillance technology leading companies, mainly European and US-based companies, did not limit themselves to serve their own governments, but went international. It emerged due to the release of many former regimes' documents following the Arab Spring that several Western companies exported surveillance technology to authoritarian governments, such as Assad in Syria and Gadhafi in Libya (see Annex II).[39]

A report published on September 2014 suggests that between 2003 and 2013, German companies alone exported "surveillance technologies to Albania, Argentina, Chile, India, Indonesia, Qatar, Kosovo, Kuwait, Lebanon, Malaysia, Morocco, Mexico, Norway, Oman, Pakistan, Russia, Saudi Arabia, Switzerland, Singapore, Taiwan, Turkey, Turkmenistan, USA, and the UAE."[40] Two of the companies in the surveillance technology sector are the Italian Hacking Team and the British-German Gamma Group. Hacking Team's flagship program, Remote Control System (RCS) "Galileo," installs malicious software on a target phone or computer that can be used to remotely monitor audio or video data. As described on the company's website:

---

[35] In December 2011, the European Commission (DG for Enterprise and Industry) instructed IHRB and Shift to develop sector-specific guidance on the corporate responsibility to respect human rights. This initiative is part of the Commission's policy on corporate social responsibility, adopted in October 2011. European Commission, "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights," <http://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf>.

[36] "Document Trove Exposes Surveillance Methods," *The Wall Street Journal*, November 19, 2011.

[37] Ibid.

[38] Tim Maurer, Edin Omanovic, and Ben Wagner, "Uncontrolled Global Surveillance Updating Export Controls to the Digital Age," *Digitale Gesellschaft*, March 2014, <www.digitalegesellschaft.de>.

[39] https://www.fidh.org/IMG/pdf/surveillance_technologies_made_in_europe-1-2.pdf

[40] Ben Wagner and Claudio Guarnieri, "German Companies Are Selling Unlicensed Surveillance Technologies to Human Rights Violators – and Making Millions," *Global Voices*, September 2014.

Take control of your targets and monitor them regardless of encryption and mobility. It doesn't matter if you are after an Android phone or a Windows computer: you can monitor all the devices.
Remote Control System is invisible to the user, evades antivirus and firewalls, and doesn't affect the devices' performance or battery life.
Hack into your targets with the most advanced infection vectors available. Enter his wireless network and tackle tactical operations with ad-hoc equipment designed to operate while on the move.
Keep an eye on all your targets and manage them remotely, all from a single screen. Be alerted on incoming relevant data and have meaningful events automatically highlighted.[41]

In July 2015, Hacking Team found itself the victim of hacking on a grand scale. Gamma International, suffered a similar hack in 2014, revealing the company's clients, capabilities and pricing.[42] Hacking Team's Twitter account was hijacked and used by hackers to release what is alleged to be more than 400 gigabytes of the company's internal documents, email correspondence, employee passwords and the underlying source code of its products. Among the documents published was the list of the company's active and inactive clients at the end of 2014. Among the company's clients, there were police agencies in several European countries, the US Drug Enforcement Administration and police and State security organisations in countries with records of human rights abuses such as Egypt, Ethiopia, Kazakhstan, Morocco, Nigeria, Saudi Arabia and Sudan. Sudan's National Intelligence Security Service was a customer given a special designation of "not officially supported." However, in a second document, an invoice for 480,000 euros to the same security service calls into question repeated denials by Hacking Team that it never did business with Sudan, which is subject to heavy trade restrictions.[43,44]

In response to concerns that Hacking Team supplied tools to repressive States, the founder of the Italian company declared to the Italian newspaper La Stampa, "We did [sell tools to Libya] when suddenly it seemed that the Libyans had become our best friends." He also admitted providing tools to Egypt, Ethiopia, Morocco and Sudan (though denied dealing with Syria). He added that "the geopolitics changes rapidly, and sometimes situations evolve. But we do not trade in weapons, we do not sell guns that can be used for years." He said that without regular updates, its tools are rapidly blocked by cyber security countermeasures.

La Stampa reports that in June 2014, the Security Council Committee, overseeing the implementation of sanctions against Sudan (established pursuant to UN Security Council resolution 1591/2005), asked the Hacking Team if the company was still selling to Sudan or if it did so in the past. The answer came following three requests on the side of the Security Council Committee, after the company stopped, in December 2014, supplying to Sudan. Hacking Team answered that, at the moment, the company was not supplying Sudan.

Since UN/EU sanctions against Sudan do not target dual-use goods and technology, the UN insisted on considering Hacking Team's products as belonging to the category "military assistance" covered by the sanctions. The debate on the legality of Hacking Team's exports was ended with the entry into force in January 2015 of Commission Delegated Regulation (EU) No 1382/2014 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.[45] The delegated act, in fact, updating the list of items subject to export authorisation,

---

[41] Hacking Team, "Remote Control System Galileo, Overview," <www.hackingteam.it>.

[42] "Hacking Team Hacked: Firm Sold Spying Tools to Repressive Regimes, Documents Claim," *The Guardian*, July 6, 2015.

[43] "Hacking Team Surveillance Technology Firm Hacked," *CBC News*, July 7, 2015.

[44] As regards to UN embargoes, see: UNSCR 1556/2004, 1591/2005, 1945/2010, 035/2012 and 2200/2015. As regard to EU embargoes, see: Council Decision 2014/450/CFSP (OJ L 203, 11.7.2014, p. 106) and Council Regulation (EC) No 747/2014 (OJ L 203, 11.7.2014, p. 1).

[45] Commission Delegated Regulation (EU) No 1382/2014 of 22 October 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, Official Journal

included the updates established by the Wassenaar Arrangement in December 2013, among which was intrusion software.[46] However, before the European regulation, the Italian competent authority, the Ministry of Economic Development (MED), imposed a catch-all clause on Hacking Team' product, on the basis of Article 4 of Regulation 428/2009 in order to control the company's exports. The catch-all clause was established on 30 October 2014 but, already on 27 November 2014, the measure was suspended (with a validity of six months) by MED.[47] According to some Italian newspapers, the decision to revoke the MED's measure came almost without surprise considering the pressure put on the competent authority by the Italian Government and the Aise (Italian External Information and Security Agency), both clients of Hacking Team.[48] Also, one day before the publication of the MED' decision to suspend the catch-all clause, a meeting between MED and Hacking Team was held following the company's request to withdraw the catch-all clause for the reason of self-defence. The document, released the following day, with MED's decision to suspend the measure, explains the constraints that Hacking Team would encounter with the catch-all clause in force. The most important reasons were stated as the following:

> *The company has very tight delivery deadlines, incompatible with the timing of administrative procedures required by the implementation of the catch-all clause;*
> *End-users are mainly governmental security and law enforcement agencies having specific needs in terms of secrecy and quick delivery;*
> *The exported product needs not to be "detected" by third parties, requiring, to this end, constant updates (camouflage software) in order to be operative and to not be neutralised by an antivirus software;*
> *Delay in deliveries (with deadlines already agreed with clients) would cause the company the payment of penalties, threatening the company's liquidity with subsequent possible failure.*

The MED' document, before stating the decision to suspend the catch-all clause, highlights Hacking Team's cooperative attitude with the MED, following the adoption of the catch-all clause, promptly presenting all required documents necessary for issuing the export authorisations.

Despite the EU Delegated Regulation No 1382/2014, which *de facto* subjected Hacking Team's product to trade controls, questions and doubts persist on the relationship between these kind of companies and their governments. It seems quite logical to raise questions about transparency and scrutiny on the supply and use of this kind of technology. It is legitimate to ask if it is acceptable that the authority that is supposed to control and verify the exports of a company is, in a way or partially, a client of the company itself. How can the government (in this specific case the MED) ensure proper trade control implementation or impose sanctions in case of violation on the company that supplies the government itself (here, in particular, the Ministry of Defence, the Aise, etc.)? What are the guarantees against the misuse of such technology by the government against its citizens? The answer given by Hacking Team's CEO, David Vincenzetti, that his company works with governments to ensure citizens' security seems inadequate in light of recent disclosures of states' mass surveillance programmes and authoritarian regimes' violation of human rights. More transparency and judiciary control are necessary.

The EU Trade Control Regime: Evolution Regarding Human Rights Protection

This section seeks to give a practical example of the difficulty of controlling MST due to three main

---

of the European Union (L 371/1), December 30, 2014.

[46] "Così il Sudan ha Messo in Crisi Hacking Team," *La Stampa*, Tecnologia, July 9, 2015.

[47] Ministero dello Sviluppo Economico, Direzione Generale per la Politica Commerciale Internazionale, Divisione IV, "Registro Ufficiale, Prot. N. 0211026 – 27/11/2014 – Uscita," November 27, 2014.

[48] "La Tecnologia di Sorveglianza Hacking Team Offerta Anche alla Gendarmeria Vaticana," *L'espresso,* July 13, 2015. See also "Hacking Team, Pansa: Gravi Danni alle Inchieste," *La Stampa*, July 30, 2015.

reasons: the rapid evolution of this technology, some systemic constrains (e.g. update of control lists) and lack of political will. The case of the EU dual-use trade control system has been chosen because it is one of the most comprehensive and advanced systems for what concerns dual-use, its emphasis on human rights issues and the protection of fundamental freedoms, and the large involvement of EU-based enterprises in the trade of MST. Despite the evolution of the EU dual-use trade control system toward a human security approach, expanding the scope of trade controls also in case of human rights concerns, the system is inadequate to prevent the misuse of mass surveillance technology.

The EU has been engaged in the protection of human rights in the field of ICTs since 2011, when the European Commission adopted the No Disconnect Strategy (NDS) to address restrictions and disruptions through ICTs, including the Internet, employed by authorities during the Arab Spring to control and repress citizens.[49] This first attempt at addressing the issues of human rights defenders facing surveillance and censorship in third countries was followed, in June 2012, by a new strategic framework and an action plan on human rights and democracy.[50] One of the main goals of this framework was to promote human rights in all EU external policies, including trade, technology and the Internet. Point 24 of the Action Plan addresses the issue of "Freedom of expression online and offline" and points out four strategies to pursue this main objective, among which: "to ensure that a clear human rights perspective and impact assessment is present in the development of policies and programmes relating to cyber security, the fight against cyber crime, Internet governance and other EU policies in this regard" and to "include human rights violations as one of the reasons following which non-listed items may be subject to export restrictions by Member States."[51]

These two strategies are particularly relevant because they relate to trade controls and in particular to the "evolution" of the EU Dual-use Regulation with regard to human rights protection. No further developments on the side of NDS have been registered.[52] Particularly useful for the protection of human rights, through trade controls, is Article 8(1) of Regulation 428/2009.[53] The Article establishes the possibility for national competent authorities to deny or require prior authorisation for export of dual-use items not listed in Annex I for reasons of public security or human rights considerations. It is quite curious to notice that, despite this provision already existing in the previous EU dual-use legislation, it has been used only in 2012 by Italy (published on September 19 (C 283/4, 19.9.2012)), when the Italian competent authority adopted a catch-all clause against Syria for public security and human rights considerations.[54] The measures aimed at controlling Public LAN database centralised monitoring system, Internet and 2G/3G services to be exported to Syrian Telecommunication Establishment (STE) in Syria.[55]

Although some Member States have mechanisms to require prior authorisations for items not listed in Annex I and some of them require systematically an authorisation for items not listed in Annex I in application of Article 8, none of the Member States has implemented Article 8 to impose an export prohibition of non-listed items.[56]

---

[49] European Commission, DG Information Society and Media Unit A3 (Internet; Network and Information Security), No Disconnect Strategy. More information on <http://europa.eu/rapid/press-release_IP-11-1525_en.htm?locale=en>.

[50] Council of the European Union, "EU Strategic Framework on Human Rights and Democracy," Luxembourg, June 25, 2012.

[51] Ibid.

[52] European Parliament, Marietje Schaake, Member of the European Parliament, Alliance of Liberals and Democrats for Europe, "Written Questions on the Follow-up on the No Disconnect Strategy," E-011923/2015, July 27, 2015.

[53] Council Regulation (EC) No 428/2009 of 5 May 2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items, Official Journal of the European Union (L 134/1) of May 29, 2009. It is worth to notice that Council Regulation 428/2009, compared to the previous dual-use Regulation, is much more comprehensive in terms of operations covered and items listed.

[54] Information note: Council Regulation (EC) No 428/2009 Setting up a Community Regime for the Control of Exports, Transfer, Brokering and Transit of Dual-use Items: Information on Measures adopted by Member States in Conformity with Articles 5, 6, 8, 9, 10, 17 and 22, Official Journal of the European Union (C 283/4), September 19, 2012.

[55] "Italy has Adopted a Catch-all Clause against Syria for Public Security and Human Rights Considerations," University of Liege, European Studies Unit (ESU), Nonproliferation News, September 19, 2012, <www.esu.ulg.ac.be>.

[56] Quentin Michel. "The European Union Dual-Use Items Control Regime: Comment of the Legislation Article-by-Article,"

Regulation 428/2009 has been subject to review since 2011. On 30 June 2011, the Commission issued a Green Paper, as established by Art. 25 of Regulation 428/2009 requiring the Commission to prepare a report on the implementation of the EU trade control system and possible area of reform.[57] The aim of the paper was to launch a broad debate concerning the EU trade control system, calling stakeholders to raise the main issues and express their views on possible evolution.

Among the challenges that the EU trade control system has to face, the Green Paper recognises new threats to security coupled with technological progress leading to increased availability of sensitive items. It also acknowledges that "technological development and the increasing number of transactions taking place put a constantly growing burden on the limited resources of export control authorities."[58] On 17 January 2013, a report on the 2011 Green Paper results was published which confirmed and developed the challenges raised by new technologies and technological development.[59] Among the new technologies, transformational technologies and cloud computing are cited, while the term "cyber-tools" appears for the first time in the Commission's documents on dual-use trade control.[60] The connection between international political events, such as the Arab Spring, and the need to prevent human rights abuses through the export control of telecommunications surveillance and internet monitoring systems are, for the first time, brought to the attention of the Commission by some Member States, some MEPs, civil society organisations and researchers. Still, in relation to computers and information security in general, some Member States, industry associations and exporters call for the introduction of new EU general authorisations in order to resolve the difficulties surrounding export of encryption technology.[61] On the issue of encryption, the document highlights that some Member States have introduced additional regulations that require advance declaration or authorisation for imports, intra EU-transfers and in-country supply, while the same items would not require any authorisation in other Member States.[62] Finally, the document points out that Member States report only few cases of additional controls introduced for reasons of security policy or human rights considerations (in application of Art.8 of Regulation 428/2009).[63]

A second step in the review process was marked by a report to the EP and the Council on the implementation of the Regulation. On the human rights issue, the report does not add much compared to the January 2013 document except for a note on national implementing measures, announcing that Italy notified the imposition of a specific national authorisation requirement on the export to Syria of certain telecommunication items not listed in Annex I for reasons of public security and human rights considerations.[64]

The Commission Communication of 24 April 2014, «The Review of export control policy: ensuring security and competitiveness in a changing world» can be considered a watershed in the EU approach to trade controls.[65] In fact, contrary to previous Commission documents, new cyber-tools and their connection

University of Liege, European Studies Unit (ESU), DUV5Rev4, August 2015, <www.esu.ulg.ac.be>.

[57] European Commission, "Green Paper: The Dual-use Export Control System of the European Union: Ensuring Security and Competitiveness in a Changing World," COM(2011) 393 final, Brussels, June 30, 2011.

[58] Ibid, p. 12.

[59] European Commission, "Commission Staff Working Document, Strategic Export Controls: Ensuring Security and Competitiveness in a Changing World - A Report on the Public Consultation Launched under the Green Paper," COM(2011) 393, SWD(2013) 7 final, Brussels, January 17, 2013.

[60] Ibid, p. 5.

[61] Ibid, p. 17.

[62] Ibid, p. 9.

[63] Ibid, p. 12.

[64] European Commission, "Report from the Commission to the Council and the European Parliament 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," COM(2013) 710 final, Brussels, October 16, 2013, p. 5.

[65] European Commission, "Communication from the Commission to the Council and the European Parliament: The Review of Export Control Policy: Ensuring Security and Competitiveness in a Changing World," COM(2014) 244 final, Brussels, April

with human rights abuses constitutes one of the main topic of focus, at the point of changing the EU approach to trade controls from military/WMD proliferation risks-based towards a "human security" approach. This new approach implies a widening of the scope of the term "strategic" as to include items and, above all technologies, which could be used for human rights abuses, although not having any direct relations with WMD proliferation concerns. As stated in the Commission Communication:

> *The Commission will consider evolving towards a "human security" approach recognising that security and human rights are inextricably interlinked. This may involve evolving towards a notion of "strategic" items addressing not only and strictly, items with possible military and WMD proliferation end-uses, but taking a wider security approach. This may also imply a clarification of control criteria to take into consideration broader security implications, including the potential effect on the security of persons e.g. through terrorism or human rights violations (…).*[66]

The Communication makes reference also to a "smart security" approach to "adjust to the transformations of dual-use items and the proliferation of new technologies."[67] Part of this approach is the development of an "EU technological reaction capacity" to ensure rapid reaction to the challenges posed by emerging technologies such as cloud computing, additive manufacturing (3-D printing), nanotechnology and to de-control items that have become obsolete or widely available commercially. In addition, to face the use of cyber-space for proliferation activities and clarification of controls of cyber-tools, the Commission considers taking actions at the multilateral level or "alternative options such as the introduction of EU autonomous lists or a dedicated catch-all mechanism."[68]

On the issue of autonomous lists, several human rights organisations asked for this solution as a possible way out from multilateral mechanisms presenting several shortcomings. In particular, a report published by CAUSE in 2014 highlights two reasons for which the EU should adopt autonomous control lists.[69] The first reason lies in the nature of the Wassenaar Arrangement, which "was established at the end of the Cold War and functions similarly to its Cold War predecessor, it focuses on risks to regional and international security and stability related to the spread of conventional weapons and dual-use goods and technologies."[70] In this sense, the WA could have a minor interest in controlling goods and technology that could be used for human rights violations or internal repression. It is more plausible that the WA places under control some surveillance technology (in particular Intrusion Software and IP Network Surveillance) because it could significantly increase the military capabilities of a State.[71] The second reason lies in the decision-making process which is time-consuming, with consensus difficult to reach due to political and technical issues.[72] In other words, the interest in including human rights issues in trade controls could not be the same at the international level, especially in a multilateral regime grouping together different countries with varying records as regards human rights.

The Commission Communication employs for the first time the term "cyber-proliferation" and makes reference to the emergence of specific cyber-tools for mass surveillance, monitoring, tracking and interception,

---

24, 2014.

[66] Ibid, p. 6.

[67] Ibid.

[68] Ibid.

[69] The Coalition Against Unlawful Surveillance Exports (CAUSE) includes: Amnesty International, Fidh, Open Technology Institute, Reporters without Borders, Digitale Gesellschaft, Human Rights Watch, Privacy International and Access.

[70] Wasseenaar Arrangement, "Introduction," <www.wassenaar.org>.

[71] Tim Maurer, Edin Omanovic, and Ben Wagner, March 2014.

[72] For example, in 2013, the WA agreed to add trojans to its list through the articulation of a control on "intrusion software," something which has proved problematic because the agreed language risks inadvertently catching too many items.

recognising that they are becoming an important dimension of export controls.[73] Finally, a relevant novelty as regards ICT control is the proposal to introduce additional EUGEAs such as for encryption to allow the export of ICT items widely used in industrial processes and operating in a highly competitive environment and for intra-company technology transfers for research and development purposes.

The European Parliament, in its legislative resolution of 23 October 2012 proposed two amendments to the Commission's proposal as regards the introduction of provisions to control unlisted items for human rights considerations.[74] One of the amendments proposed concerned the wording of Article 8(1) and precisely, the EP proposed to replace the word "may" with the word "shall":

> *A Member State may prohibit or impose an authorisation requirement on the export of dual-use items not listed in Annex I for reasons of public security or human rights considerations.*

It is reasonable to think that the EP, by introducing the modal verb "shall" instead of "may" wanted to give a more mandatory tone to the provision, reducing Member States' marging of appreciation.

The second major amendment proposed by the EP and not introduced in the Regulation was the insertion of a paragraph to Article 4, which establishes the possibility of catch-all clauses. The amendment proposed by the EP was that the following paragraph be inserted:

> *An authorisation shall also be required for the export of dual-use items not listed in Annex I if the exporter has been informed by the authorities referred to in paragraphs 1 and 2, or by the Commission, that the items in question are or may be intended, in their entirety or in part, for use in connection with a violation of human rights, democratic principles or freedom of speech as defined in the Charter of Fundamental Rights of the European Union, by using interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of internet use, such as via monitoring centres or lawful interception gateways.*[75]

It is evident that the EP, already in 2012, recognised the importance of covering the control of items and technologies that could be used in violation of human rights and, going even further, the EP tried to insert a mechanism also for the protection of democratic principles and freedom of speech as defined by the Charter of Fundamental Rights of the EU- a human rights/democratic principle catch-all clause identifying the type of items and technologies that could be included in such a provision (interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of internet use, such as via monitoring centres or lawful interception gateways). A pending question is why the Commission only made reference to such risks and related measures in its Communication in 2014 and why the EP's proposals for amendment were not inserted in the final Regulation.

Proceeding with the evolutionary process of the EU Dual-use Regulation as regards human rights protection, on 30 December 2014, Commission Delegated Regulation (EU) No 1382/2014 entered into force updating Annex I as to include modifications adopted by export control regimes in 2011, 2012 and 2013.[76] This

[73] European Commission, COM(2014) 244 final, Brussels, April 24, 2014, p. 3.

[74] European Parliament legislative resolution of 23 October 2012 on "the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, COM(2011)0704 – C7-0395/2011 – 2011/0310(COD), October 23, 2012.

[75] Ibid.

[76] European Commission, "Commission Delegated Regulation (EU) No 1382/2014 of 22 October 2014.

delegated Regulation has particular importance as regards human rights protection and mass surveillance technology control because it inserts the Wassenaar Arrangement's December 2013 updates, including some "Intrusion Software" and "IP Network Surveillance Systems."

As for Annex I of the EU Dual-Use Regulation, "Intrusion software" falls within Category 4, (Computers Systems, Equipment and Components), control entry 4A005, while "IP Network Surveillance Systems" fall within Category 5 (Telecommunications systems, equipment, components and accessories), control entry 5A001. A white paper released by Access in March 2015 makes a technical analysis of these two categories of items included in the WA Control list and raises some important points, especially at the level of language used in the definition and the scope covered.[77]

The main concerns emerging from the analysis are the following:

As regards "Intrusion software,"the control is not designed to solve the totality of threats to information security and privacy[78] (for example, it does not regulate the ample market for commercial malware that is sold to the general public and it does not attempt to holistically control the broad range of software that may be used to compromise user data); and "the definition of control is too broad as to create fear that the controls regulate commonplace research, instead of concerns about missed technologies."

As regards IP Network Surveillance, the paper states that "there is no indication that the Wassenaar Arrangement language would apply to the deep packet inspection (DPI) equipment or lawful interception systems that have routinely evoked controversy when exported to countries that violate human rights.... The definition of the IP Network Surveillance is too narrow and may be reflective of the uncertainty that export control authorities face in asserting administrative burden on the sale of dual-use network equipment (frequently used for censorship, but also commonplace in networks for caching of content, mitigating security threats and other purposes, even in countries with human rights challenges)."[79]

However, the paper underlines that:

> *The exemptions under both Intrusion Software (for debuggers, software reverse engineering, digital rights management, and asset recovery) and IP Network Surveillance (marketing and network management) appear to be narrowly-defined and are unlikely to present significant short-term risk of re-labelling by companies that may want to apply avoid scrutiny*[80].

It seems that the 2013 WA updates on surveillance technology are the results of two different proposals: a UK proposal focused on "advanced persistent threat software and related equipment (offensive cyber tools) and a French proposal for the control of IP network surveillance systems.[81]

The term used "intrusion software" (language finally adopted by the WA plenary in December 2013) is defined as:

---

[77] Collin Anderson, "Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies", March 9, 2015, available at: http://cda.io/r/ConsiderationsonWassenaarArrangementProposalsforSurveillanceTechnologies.pdf.

[78] Ibid. p. 11.

[79] Ibid. p. 5.

[80] Ibid. p. 7.

[81] Tim Maurer, Edin Omanovic, and Ben Wagner, "Uncontrolled Global Surveillance Updating Export Controls to the Digital Age," *Digitale Gesellschaft*, March 2014, <www.digitalegesellschaft.de>.

Software specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer or network capable device, and performing any of the following:
a. The extraction of data or information, from a computer or network capable device, or the modification of system or user data; or
b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.
Points (a) and (b) captures two different aspects of the technology that will be subject to control. Point (a) covers the exfiltration of data from the victim's system such as microphone or camera streams and it also includes software that changes files on the victim's machine. Point « b » defines the mechanism by which commercial malware typically infects its victim's devices (this is the exploit mechanism that the surveillance product takes advantage of).

The actual controls are defined as:

4. A. 5. Systems, equipment, and components therefor, specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software".
4. D. 4. "Software" specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software".
[4. E. 1.] c. "Technology" for the "development" of "intrusion software."

Two main considerations (strictly related) can be done on the definition of controls. The first is that intrusion software per se is not subject to controls; the second consideration is that controls target the components that stay under direct control of the purchaser, leaving outside any component that would end up on a victim's end-user device. The logic behind this definition of control is clear and it is to target those who purchase intrusion software and seek to target others, not those who are infected with it. Without this logic, the risk would be a violation of export controls by the targeted user carrying an infected device, especially if travelling to another country. As a consequence, software to achieve these activities must reside off the victim's device, while the intrusion software itself must reside on the device.[82]

Regarding IP network surveillance systems, these are defined as:

5. A. 1. j. IP network communications surveillance systems or equipment, and specially designed components therefor, having all of the following:
1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):
Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));
Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and
Indexing of extracted data; and
2. Being specially designed to carry out all of the following:
Execution of searches on the basis of 'hard selectors'; and
Mapping of the relational network of an individual or of a group of people.

The concern here is that the definition of controls targets a very narrow category of products, risking to fail to cover some of the systems of greatest concern, as already stressed above.[83] As explained, surveillance technology remains an issue for several reasons. The first is that not all states are members of the WA and,

[82] Ibid.
[83] Ibid.

even if this was the case, there is no legally-binding obligation for states to implement decisions taken in the multilateral forum. Second, although all WA members are willing to implement trade controls established at the international level (as it is the case for EU Member States implementing WA updates through the EU Dual-use Regulation, legally-binding and directly applicable to/in all EU Member States), competent national authorities in each state do not necessarily have the same interpretation of the provisions, as stressed by MEP Schaake in her oral question on export controls and Hacking Team, debated in the European Parliament on 5 October 2015.[84] The result is a very fragmented regulatory system leaving too much space for violations and abuses.

In June 2015, a report was published by the EP Committee on Foreign Affairs.[85] The Rapporteur highlights the dual-use nature of information technology, especially software, which plays an increasingly important role in enabling and ensuring the fulfilment and full respect for human rights and fundamental freedoms by expanding the scope of freedom of expression, of association and assembly and access to information. But, at the same time, the same tools can be used for the violation of human rights and fundamental freedoms through surveillance, censorship, unauthorised access to devices, jamming, interception and tracing and tracking of information and individuals. The report also points out the increasing role assumed by private actors in assessing the legality of content and in developing cyber-security systems and surveillance systems in the absence of a legal basis that rests on the precepts of necessity, proportionality, and democratic and judicial oversight. The role of EU-based companies is also recognised as having an important share of global market in ICTs, in particular in the field of surveillance, tracking, intrusion and monitoring technology exports. At the same time, the responsibilities of some EU-based companies is clearly recognised as having contributed to human rights violations worldwide through the export of such technology. Member States are also called into question as far as their complicity in the NSA's mass surveillance programmes "as revealed by Edward Snowden, has caused serious damage to the credibility of the EU's human rights policy and has undermined global trust in the benefits of ICTs."[86] The EP report, as many other documents and articles, establishes a direct link between violation of human rights and fundamental freedoms counter-terrorism measures used as pretexts for such violations. To this end, the EP insists that such measures be pursued strictly in line with the rule of law and human rights standards.

To react against such a negative trend, the report asks for several actions to be taken. One is the inclusion of clauses in agreements with third countries that would promote, guarantee and respect digital freedoms, net neutrality, uncensored and unrestricted access to the Internet, privacy rights and the protection of data."[87] Other actions are, for example, to ensure greater transparency in the relationship between internet service providers and governments; the implementation and monitoring of EU regulations and sanctions relating to ICTs; the public exclusion of companies engaging in ICTs exports with detrimental effects on human rights, and the introduction of "end to end" encryption standards. In the specific framework of the dual-use policy review, the EP, however, calls on the Commission to pay attention to avoid any measures that could inhibit legitimate research or access to and exchange of information and that could have a "chilling effect" on individuals or SMEs. To avoid this side effect, the EP proposes, for example, the use of EU General Export Authorisations for dual-use research. Finally, the report calls for an end to mass surveillance, considering that the issue must be addressed and stopped.

The EP resolution of 8 September 2015, which transposes word by word the report, addresses the mass surveillance issue on two dimensions: the internal dimension involving the surveillance of EU citizens and

---

[84] European Parliament, Marietje Schaake, Member of the European Parliament, Alliance of Liberals and Democrats for Europe, "Oral Questions on Export Controls and Hacking Team," (O-000094/2015), September 3, 2015.

[85] European Parliament, "Human Rights and Technology: The Impact of Intrusion and Surveillance Systems on Human Rights in Third Countries," 2014/2232(INI), June 6, 2015.

[86] Ibid, p. 8.

[87] Ibid, p. 10.

the subsequent issue of violation of fundamental freedoms and on the external dimension, by addressing the problem of surveillance technology export controls.

This EP resolution, during the dual-use policy review period, can be considered a reminder of the challenges posed by information and digital technology. But it is also a warning, on the side of the democratically elected institution, to governments and to public opinion in general to pay attention to the kind of society being built. In fact, although the EP resolution is meant to address the issue of the impact of intrusion and surveillance systems on human rights in third countries, half of the report focuses on the impact of surveillance technology inside the EU, on EU citizens "attacked" not by terrorists but by their governments.

Conclusion

This paper analysed the issue of mass surveillance technology on two dimensions: states' internal dimension involving the surveillance of citizens and the subsequent issue of violation of fundamental freedoms (such as the right to privacy and data protection), and the external dimension, by addressing the problem of surveillance technology export control, especially to countries likely to use such technology to violate human rights. It emerged that following the "Snowden's datagate scandal" on mass surveillance programmes, many states undertook inquiries and adopted measures that, in some cases, were meant to regulate the use of mass surveillance technology. It appeared, in fact, that surveillance technology used by security and law enforcement agencies, in order to fight terrorism, was not always used following the principle of proportionality and necessity, giving birth to the phenomenon of mass surveillance to the detriment of targeted surveillance subject to prior judiciary control.

On the external level, rapid technological development and a certain dose of inertia on the side of political élites left the legal framework deprived of adequate instruments to control the export of surveillance technology. The consequence has been a rapid development of private industry in supplying such technology to governments all over the world, sometimes regardless of any human rights implications.

In this intricate context, the EU started to develop a trade control policy more inclusive of a "human security" approach. Especially through the review of the Dual-use Regulation, since 2011 the EU widened the scope of its trade control system to include goods and technologies that could be used in violation of human rights. This is the aim and raison d'être of article 8(1) of EU Regulation 428/2009 establishing the possibility for national competent authorities to deny or require prior authorisation for export of dual-use items not listed in Annex I for reasons of public security or human rights considerations. Another step forward has been the entry into force of Commission Delegated Regulation (EU) No 1382/2014 of 22 October 2014, which updated Annex I to include modifications adopted by export control regimes in 2011, 2012 and 2013 and, in particular, December 2013 Wassenaar Arrangement's updates, including some "Intrusion Software" and "IP Network Surveillance Systems." Despite this progress, several issues remain that raise questions about the effectiveness of trade controls in preventing the violation of human rights and, in general, the capacity of trade control systems to adopt the human security approach.

The first issue concerns the nature of existing multilateral export control regimes, especially the WA, which does not take into account the control of goods and technologies for human rights concerns. This reality is particularly problematic for implementation of the EU dual-use control list, which being an implementer of multilateral export control regimes' lists, is "limited" to control items decided on the international level. Until present, the idea of an EU independent list is not being considered. The catch-all clause mechanism has been the only way include the possibility of controlling items on the grounds of human rights concerns

but is just a possibility and the implementation is up to Member States.[88]

A second issue regards suppliers of surveillance technology that, given their role as governments' suppliers, sometimes seem to consider themselves (or are allowed to consider themselves as) "above the law," invoking their role of "security providers." In fact, whether they have been operating in a grey zone where surveillance technology has not always been clearly subject to trade controls, or under strict and transparent legislation on surveillance technology trade controls, the privileged relationship that some companies have with their own governments (in the form of of technology suppliers) may not be a warranty of fairness and legality. Would a government sanction the a company for trade controls violations, when the same firm is that governments' supplier?

There is still hope that the current dual-use Regulation review period will take into account recent EP resolutions and human rights defenders' requests to strengthen the EU trade control system in a way to be more in line with EU values and principles that, from the very beginning, inspired its construction and integration. One last wish is that democratic societies all over the world will remember Benjamin Franklin's famous quote, "Those who desire to give up freedom in order to gain security will not have, nor do they deserve, either one."

[88] It is worth noting that the implementation of catch-all clauses in the EU could be problematic and create problems at the level of fair competition. The issue of competition, but at the international level, was raised also by the Italian company Hacking Team affirming that if it was hindered by the competent authority to export, one of its main competitor (the Israeli company Maglan) would have won, adding that there is a lot of difference between a technology developed by an Italian company under the supervision of the MED and an Israeli one that could be designed with multiple and obscure purposes.