Uncontrolled Global Surveillance

Updating Export Controls to the Digital Age

By Tim Maurer, Edin Omanovic, and Ben Wagner

March 2014

Executive Summary

In 2011, the Wall Street Journal reported "the annual value of the retail market for surveillance tools has increased from 'nearly zero' in 2001 to around $5 billion a year." The Arab Uprising and the fallen regimes' documents that became public in the aftermath shed light on this growing industry. Some authorities employed this technology for political control and to facilitate internal repression, the suppression of the media and civil society, and other violations of fundamental human rights. Technologies were found to have been exported to authoritarian governments, such as Assad's Syria and Gadhafi's Libya with companies in the United States, France, and the United Kingdom facing legal challenges subsequently. It became clear that, while surveillance technology can have legitimate uses, it can also be abused for nefarious purposes and become a powerful facilitator of oppression.

This paper focuses on export controls as one policy option to address this problem. A key finding of this paper is that existing export control regulations have become out-dated and have not kept up with new technology. This report provides an in-depth policy and technological analysis of existing export controls as they relate to surveillance technology. Given the importance of a multilateral approach for export controls to be effective overall, it focuses on the export control regimes in three countries - Germany, the United Kingdom (UK), and the United States (US) - and was conducted as a joint project by three organizations in these three countries.

At the same time, government regulation can have a negative impact on technology, innovation, and trade. The "Crypto Wars" of the 1990s, a multiyear struggle to loosen export controls on encryption initially on the munitions list in the US, exemplified how broad-brush and poor policy related to export controls and technology can do more harm than good. This report is therefore based on a technical analysis incorporating invaluable input from technologists to flag concerns as well as a targeted and careful policy analysis to avoid negative consequences bearing in mind the lessons learned from the Crypto Wars.

Introduction[i]

In 2011, the Wall Street Journal reported "the annual value of the retail market for surveillance tools has increased from 'nearly zero' in 2001 to around $5 billion a year."[1] This explosion of demand is the result of three important trends that have shaped surveillance policy and practice across the last 15 years. First, the 9/11 terrorist attacks were largely blamed on intelligence failures and the attacks in Bali, Madrid, London, and Mumbai further underlined the need for better intelligence and intelligence-gathering capabilities. Second, new technologies are generating vast quantities of data, posing novel challenges for legal and regulatory frameworks, but also creating unprecedented opportunities for law enforcement and intelligence agencies around the world to use that data. And third, governments increasingly rely on the private sector and commercial technologies to keep up with technological changes and demands.[2]

Surveillance technology has legitimate uses, but it can also be abused for nefarious purposes. While surveillance tools can serve important ends for law enforcement agencies in states with strong human rights protections and respect for the rule of law, they can also be powerful facilitators of oppression in others. Data relating to entire populations, groups, and individuals can be abused by authorities for political control and facilitate horrific instances of internal repression, the suppression of the media and civil society, and other violations of fundamental human rights. "Technologies are being created and customized with the explicit purpose of helping repressive regimes track down, detain, torture and murder people," aaccording to the Electronic Frontier Foundation on a case that was recently dismissed by a court referencing export controls.[3]

The Arab Uprising represented a significant turning point. Through the release of former regime documents, the upheavals shed light on this growing industry and the complicity of Western companies in exporting technologies to authoritarian governments, such as Assad's Syria[4] and Gadhafi's Libya.[5] These revelations spurred a flurry of research[6] and media interest,[7] primarily focused on identifying which technologies were being used for surveillance and in which countries. As more evidence emerged highlighting the role surveillance technology plays in facilitating human rights abuses, civil society groups and policy makers began seeking avenues to bring pressure to bear on the companies developing and selling it. Companies in the US,[8] France,[9] and the UK[10] faced legal challenges, while calls for companies to self-regulate also gained traction.

This paper focuses on a crucial policy option to address this problem: export controls. A key finding is that existing export control regulations have become out-dated and have not kept up with new technology. Export control measures are a well-established instrument governments use to ensure transfers of certain items are in line with their foreign policy and security objectives as well as international obligations. They allow government authorities to review which items are exported, and to whom. Depending on the level of control, exporters might be required to notify authorities before shipment or apply for a license; a license can then be granted or refused on specific grounds. The actual items that fall under the scope

[i] The authors would like to thank several individuals for their guidance and assistance, namely Collin D. Anderson, Kevin Bankston, Mark Bromley, Brian Duggan, Fukami, Danielle Kehl, Heinrich Köllisch, Jordan McCarthy, Robert Morgus, Nick Russo, Dan Staples, Volker Tripp, and Seamus Tuohy. In addition, we appreciate the input we have received from government representatives and company officials. This paper does not necessarily reflect the views of these individuals.

of export controls can be decided either multilaterally or unilaterally.

Policy makers and civil society groups have called for governments to regulate the export of surveillance technology to end users with dubious human rights records. The adoption of effective export controls for such dual-use technologies will ensure that they are not exported to end users where a risk exists that they could be used to facilitate human rights abuses.

Several governments and institutions have imposed export controls on some types of surveillance technologies or have made efforts to do so. Given the lack of international, coordinated action, however, such moves have been piecemeal and largely ineffective. In fact, a US court recently dismissed a case and specifically referenced the lack of US trade regulations regarding technology as part of the problem.[11] Clearly, there has been insufficient analysis on the policy dimension of this problem and to what degree existing export control regulations cover this technology.

This report addresses the existing gap and provides policy and technological analysis of export controls relating to surveillance technology. This paper focuses specifically on the export control regimes in three countries - Germany, the UK, and the US - and was conducted jointly by three organizations in these three countries.

This project was deliberately designed to be multinational. Unilateral controls are important for a government to align its export control policy with its human rights and foreign policy but the controls' effectiveness is limited if other countries do not implement similar controls. A larger group of states, those with the biggest market shares, therefore needs to act together to maximize the effectiveness of an export control regime which is why this project focused on Germany, the UK, and the US. There will be some countries with a significant market share that might not follow this example. However, for democratic and human rights promoting states it is important to lead by example as outlined in US crime control policy: "The judicious use of export controls is intended to deter the development of a consistent pattern of human rights abuses, distance the United States from such abuses…these controls are not based on the decisions of any multinational export control regime and may differ from controls imposed by other countries."[12]

An important caveat concerns export controls vis-à-vis technology. The authors are aware of the negative impact that government regulation can have on many areas of technology, innovation, enterprise, and trade. The "Crypto Wars" of the 1990s, a multiyear struggle to loosen export controls on encryption initially on the munitions list in the US. They exemplified how broad-brush and poor policy related to export controls and technology can do more harm than good. As a result of this and other restrictive regulatory measures on the security industry by states, the technical community has become very wary of export controls. Surveillance is a broad term and the products used for it are technically complex. Not all products that can be used for surveillance should or can be made subject to export controls. This report is therefore based on a technical analysis incorporating invaluable input from technologists to flag concerns as well as a targeted and careful policy analysis to avoid negative consequences bearing in mind the lessons learned from the Crypto Wars. It is clear that any controls in this area must be specifically clear and carefully crafted as well as accompanied by regular updates and feedback loops allowing input from non-governmental sources.

Moreover, in addition to the recommendations outlined in this report specific to surveillance technology, the authors also believe that the existing controls on encryption need to be updated

and further loosened so individual users can better protect themselves against surveillance and other forms of electronic snooping. While encryption controls have been used by the UK government to control FinFisher, Gamma International's primary surveillance software, encryption controls should not be used as a substitute for stand-alone controls for surveillance technology. Mixing the two different types of controls will only create significant challenges in the future because encryption controls are likely to be further relaxed in the future. New controls should be established and implemented separately and independently from the encryption controls.

This paper is divided into five sections. The first three sections outline the national export controls regimes in the US, the UK, and Germany, including existing provisions relating to human rights and surveillance technologies. Exports from these three countries constitute a significant share of this growing industry. Promoting human rights is also among each country's foreign policy priorities. Together, they can drive the policy and regulatory changes needed to update existing export controls.

The fourth section discusses the European Union's (EU) role, adding an additional dimension to the UK and German export control regulations. The EU as an actor in this field is particularly important given the policy-making and legislative role it plays in the field of trade across its member states. Further, it is widely documented that European companies have been responsible for providing much of the surveillance capabilities of authoritarian regimes across Northern Africa and the Middle East in the wake of the Arab Uprising.

The fifth section consists of two parts. The first offers a short description of the relevant existing export controls regime, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (Wassenaar Arrangement). It is a forum for states to agree which specific technologies should be subject to export control for regional and international security and stability reasons. The second section provides an analysis of the 2013 Wassenaar Arrangement changes adopted in December 2013 when the 41 participating states took an important step and agreed to establish new controls relating to "intrusion software" and "Internet Protocol network surveillance systems".

These 2013 changes now need to be implemented by participating states. This report offers recommendations on how to implement the new controls while avoiding unintended negative consequences. It is important to note that the Wassenaar Arrangement does not obligate states to assess the human rights impact of transfers of such goods. In addition to ensuring technologies are within states' scope of control, they must therefore also agree on strong commitments to appropriate criteria related to human rights when assessing export license applications for surveillance technologies.

At the same time, the recent changes to the Wassenaar Arrangement are only a first step to examine existing controls in the context of the emerging surveillance industry and to update them. A range of technologies that can be abused for this purpose must be studied further. Encouraging input from non-governmental policy makers, civil society groups, and the surveillance industry will be crucial to inform this process and to minimize unintended negative consequences. In order to contribute to this process in the future especially as new technology is developed at a pace requiring continuous input for controls to remain up-to-date and well-crafted, it is important for all stakeholders to understand how specific technology is made subject to export controls.

(1) US EXPORT CONTROLS – a "byzantine amalgam"

The US is the world's second largest exporter and the world's number one importer of goods and services.[13] It is also the world's biggest exporter of arms with a 30 percent share of global arms transfers from 2008-2012.[14] The US export control regime regulates a small percentage of overall US exports. According to the US Department of Commerce's Annual Report to Congress for Fiscal Year 2013, only 1.7 percent of overall US exports were licensed items (0.3%) or items subject to controls but exportable pursuant to a license exception (1.4%).[15] The regime derives from the US Constitution itself, which states that, "Congress shall have power…to regulate Commerce with foreign Nations". Congress has used this authority to establish several export control laws.[16]

Unlike Germany and the UK, the US neither has a single agency in charge of administering these controls nor a consolidated list of items subject to controls. According to Secretary of Defense, Robert Gates, the US export control system is a "byzantine amalgam of authorities, roles, and missions scattered around different parts of the federal government."[17] Two departments are the lead agencies: the US Department of State administers arms controls through the US Munitions List (USML) and the US Department of Commerce oversees dual-use items through the Commerce Control List (CCL). Companies must first determine whether their export is regulated by Commerce or State, and then follow the applicable regulations. State and Commerce also serve as licensing agencies complemented by the Treasury. Moreover, in the US multiple agencies are involved in enforcement whereas the customs departments are the sole agencies in charge in Germany and the UK.[18] [ii]

Generally, export control policymaking in the US tends to be quite insular. It is mostly decided through intra-governmental processes with a limited number of outside experts influencing policy developments, mostly export control lawyers, private consultants usually with previous experience in export controls working for the government, and specialized associations. The US Department of Commerce relies on the input from eight Technical Advisory Committees, comprised of representatives from industry and government, focused on dual-use items and technology.[19] They include the Emerging Technology and Research Advisory Committee, the Information Systems Technical Advisory Committee, the Regulations and Procedures Technical Advisory Committee, and the Sensors and Instrumentation Technical Advisory Committee. In addition, companies and other members of the public can provide formal feedback in response to requests for comments and informally at conferences and meetings.

Legislative Framework for US Export Controls

Congress has delegated its aforementioned constitutional authority to regulate "commerce with foreign nations" to the executive branch through a number of legal acts, namely the Arms Export Control Act (AECA), the Export Administration Act (EAA), and the International Emergency Economic Powers Act (IEEPA). It is important to note that the EAA has been expired since 2001 (see Figure 1). However, the actual Export Control Regulations (EAR), which are essentially the implementation of the law, created under the EAA remain in place. They continue to be

[ii] It is important to bear in mind that the export control regulations discussed in this paper are different from sanctions regulations. The former cover exports to any country generally, the latter focus on specific sanctioned countries.

Figure 1

LEGISLATION	
Statute:	Arms Export Control Act (AECA)
Regulation:	International Traffic in Arms Regulations (ITAR)
List:	US Munitions List (USML)
INSTITUTION	
Agency in charge:	US State Department
Lead unit within agency:	Directorate of Defense Trade Controls (DDTC)
LEGISLATION	
Statute:	Export Administration Act (EAA) (expired since 2001)
Regulation:	Export Administration Regulations (EAR)
Currently in place under authority of International Emergency Economic Powers Act (IEEPA)	
List:	Commerce Control List (CCL)
INSTITUTION	
Agency in charge:	US Department of Commerce
Lead unit within agency:	Bureau of Industry and Security (BIS)

in effect under authority exercised pursuant to IEEPA.[20] Under the latter, criminal penalties can be up to 20 years in prison and/or up to $1 million in fines. Civil penalties are set at $250,000 or twice the amount of the violating transaction.[21]

According to the Congressional Research Service, DDTC's budget was $11.6 million in FY2012. Its staff consisted of 81 members and it processed 82,095 export license applications. BIS processed 23,229 export license applications in FY2012 worth approximately $204.1 billion. Less than one percent of these applications were denied, some of those that were approved included conditions. BIS has a staff of some 390 full-time employees.[22] In FY2013, BIS processed 24,782 export license applications of which it denied 177 (less than one percent).[23]

Other departments involved in this interagency process include the US Department of Defense which assists the US State Department and US Department of Commerce in administering their respective controls, the US Department of Homeland Security which focuses on enforcement, and the US Department of Justice which conducts criminal investigations. A company can request a commodity jurisdiction determination from the State Department in cases where it is unclear what regulation an export falls under.

Structure of US export controls and implementation

The Department of Commerce's jurisdiction covers all exports subject to the EAR which includes US origin items and foreign items with a US item component and technology. It is important to note that these controls apply to these items wherever they are located in the world and also includes "deemed exports", the release of controlled technology to foreign persons in the US.[24]

Exports considered potentially sensitive are assigned specific export control classification numbers (ECCNs) and might require a license depending on the type of item, end user, and destination. Once a license application has been submitted, the decision-making process is supposed to be completed within 90 days including

feedback from other agencies as illustrated in Figure 2 (reproduction).[25] Generally, the ECCNs apply to items that are not "publicly available" and that are not exclusively subject to other regulations. Similar to the commodity jurisdiction determination, companies can request a commodity classification from the US Department of Commerce to determine what category the export belongs to.

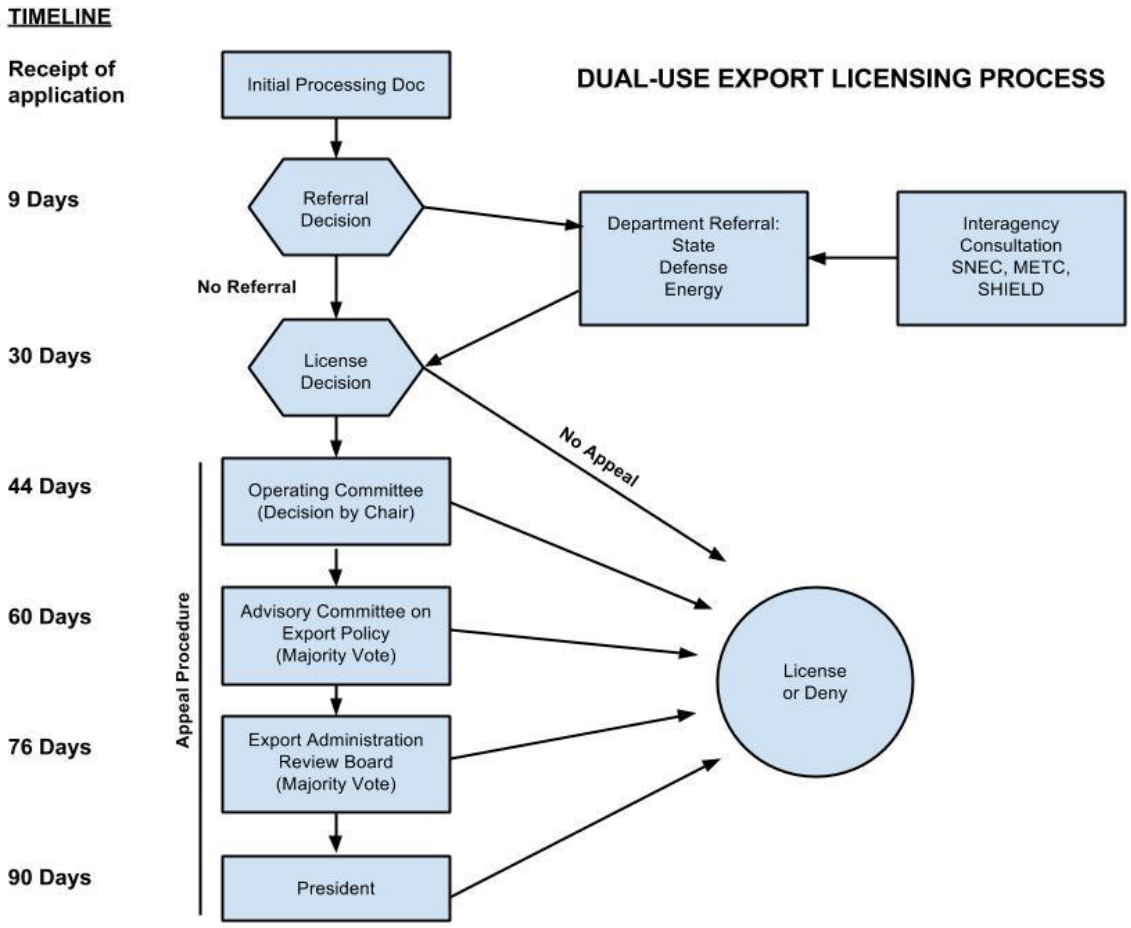
For all other items, the US Department of Commerce created a special classification category, called "EAR99", stating that

"If your item falls under US Department of Commerce jurisdiction and is not listed on the CCL, it is designated as EAR99. EAR99 items generally consist of low-technology consumer goods and do not require a license in many situations."[26]

EAR99 exports usually fall into the category of "No License Required" except if they are going "to an embargoed country, to an end-user of concern, or in support of a prohibited end-use."[27]

The US export control regime corresponds with the multilateral export control lists but also includes a number of stricter unilateral controls.[28] The US Department of Commerce reviews dual-use exports for a variety of reasons which are sometimes broadly divided into national security, foreign policy, or short supply. The US Department of Commerce provides this more detailed outline: The second digit of an ECCN identifies the reason

Figure 2



for control which can be

- 0: National Security reasons (including Dual Use and Wassenaar Arrangement Munitions List) and Items on the Nuclear Suppliers Group Dual Use Annex and Trigger List
- 1: Missile Technology reasons
- 2: Nuclear Nonproliferation reasons
- 3: Chemical & Biological Weapons reasons
- 5: Items warranting national security or foreign policy controls at the determination of the US Department of Commerce.
- 6: "600 series" controls items because they are items on the Wassenaar Arrangement Munitions List or formerly on the USML.
- 9: Anti-terrorism, Crime Control, Regional Stability, Short Supply, UN Sanctions, etc.

If the number "9" appears as the second or third digit it identifies a unilateral control. [29]

The majority but not all of the reasons and to which countries they apply is summarized in the "Commerce Country Chart," provided by the Department of Commerce.[30] This list provides an outline for the level of control depending on the end destination. The full list of reasons is:

- AT Anti-Terrorism
- CB Chemical & Biological Weapons
- CC Crime Control
- CW Chemical Weapons Convention
- EI Encryption Items
- FC Firearms Convention
- MT Missile Technology
- NS National Security
- NP Nuclear Nonproliferation
- RS Regional Stability
- SS Short Supply
- UN United Nations Embargo
- SI Significant Items
- SL Surreptitious Listening

The US export control system is currently undergoing a major reform effort under the President's Export Control Reform Initiative (ECR) "to address the increasing challenges posed by an outmoded export control system created during the Cold War".[31] The ECR was first announced by President Obama in 2009.[32] The goal is to create the "four singularities": a single licensing agency, a single control list, a single enforcement structure and a single IT system.[33] US administration officials often describe the goal of the ECR as "higher fences around fewer items". "Fewer items" means the transfer of items from the stricter USML to the more flexible CCL while creating "higher walls" by clarifying existing controls and decreasing ambiguity.[34]

Harmonizing and consolidating the USML and CCL has been a focus in order to reduce overly broad generic controls in favour of more concrete specifications. The agencies will also being using a single IT system called USXports currently used by both the US Department of Defence and the US Department of State with the US Department of Commerce joining in 2014. The ultimate goal is to create a single licensing agency.[35] The export control reform process has provided more opportunities for outsiders to provide input and feedback on export control policy to the government. Some of the changes were criticized by the American Bar Association's Center for Human Rights and the Open Society Foundations because of the potential negative human rights implications of this process.[36] At the same time, encryption controls are being loosened as part of the reform initiative.[37]

US export controls and human rights

In the US, some argue that US export controls are overly restrictive with negative effects on competition. Others say that national security and foreign policy trump economic concerns. According to the Congressional Research Service, to this latter group, "reform should be concerned less with the abilities of US industry to export and more with effective controls placed on potential exports to countries that threaten the security of the United States, terrorists, violators of human rights, and proliferators of weapons of mass destruction."[38]

National security and economic concerns are the main drivers of US export control decisions, but foreign policy controls also include a human rights component. For example, "The EAR restrict the exports of specially designed implements of torture and equipment designed for the execution of humans".[39] Moreover, the BIS's 2014 Report on Foreign Policy-Based Export Controls outlines a general policy of denial for license applications for exports of crime control items for countries with a pattern of human rights violations or experiencing civil disorder. For other countries, the decision is weighed on a case-by-case basis with the US Department of State reviewing license applications, including considering whether a denial would help deter human rights abuses or signal that the US opposes such behaviour.[40]

The respective paragraph of the EAR (§ 742.7 – Crime control) specifically mentions:

> (a) License requirements. In support of US foreign policy to promote the observance of human rights throughout the world, a license is required to export and reexport crime control and detection equipment, related technology and software. . .
>
> (b) Licensing policy. Applications for items controlled under this section will generally be considered favourably on a case-by-case basis unless there is civil disorder in the country or region or unless there is evidence that the government of the importing country may have violated internationally recognized human rights. The judicious use of export controls is intended to deter the development of a consistent pattern of human rights abuses, distance the United States from such abuses and avoid contributing to civil disorder in a country or region.
>
> (d) US controls. In maintaining its controls on crime control and detection items, the United States considers international norms regarding human rights and the practices of other countries that control exports to promote the observance of human rights. However, these controls are not based on the decisions of any multinational export control regime and may differ from controls imposed by other countries.[41]

The report highlights that "US-unilateral controls restrict human rights violators' access to US-origin goods and provide important evidence of US support for the principles of human rights". The report also points out that "any adverse effect of these controls on the economy of the United States, including on the competitive position of the United States in the international economy, does not exceed the benefit to US foreign policy objectives." Importantly, the US government considers this policy to be effective at achieving its foreign policy goal even though only a few other countries have similar regulations in place.

This is underlined by the fact that the foreign availability provision, the availability of a product and ability for it to be purchased from another country, does not apply this section of the EAA. In fact, Congress has recognized the importance of these controls for US foreign policy and human rights policy.[42] Similarly, a 2013 report outlines that human rights considerations have influenced export control decisions under the USML and the "Leahy Law" explicitly prohibits military assistance to security forces of a foreign country that commit human rights violations.[43]

The US Department of State plays a key role for human rights considerations to influence export licensing decision-making. This includes information outlined in the US Department of State's annual Country Reports on Human Rights Practices which includes a section on Internet Freedom.[44] For example, the 2012 edition for Syria states that the government

> routinely monitored Internet communications, including e-mail (see section 2.a.). Local human rights groups reported that activists' computers were often infected with malware…Human rights activists believed the government often attempted to collect personally identifiable information of activists on the Internet to coerce or retaliate against them. Activists reported that authorities forced them to provide the passwords to their e-mail and social media accounts, and government supporters subjected their Web sites and accounts to attacks.[45]

The report on Bahrain is another example where the State Department provides information that can help to assess the potential risk of a technology being abused depending on the end user and destination. It outlines that

> Reports also indicated the government used computer programming to spy on political activists and members of the opposition inside and outside the…The government restricted Internet freedom and monitored individuals' online activities, including via social media leading to legal action and punishment of some individuals during the year… According to reports published by Bloomberg News, an unknown source sent spyware to activists via e-mail in April and May. According to the press report, the e-mails, which appeared to come from close associates, were sent from the hacked accounts of activists' associates and contained messages about events in the country with malware disguised as hyperlinks. The report indicated the spyware could harvest sensitive personal data from targeted computers. The spyware producer stated it did not sell its program in the country.[46] (The Bloomberg News report focused on Gamma and FinFisher.[47])

Existing US export controls relating to surveillance technology

Crime controls are a precedent and important example for the human rights considerations that are part of the US export control system generally. In addition, existing ECCNs include a few, limited provisions regarding surveillance technology outlined in Figure 3.[48]

It is noteworthy that while the surreptitious listening controls focus on communications by

terrorists, the US government also mentions that their purpose is to "promote the protection of privacy of oral, wire, or electronic communications".[49] According to §742.13 of the EAR surreptitious listening controls require a license for all destinations and therefore do not appear separately on the Commerce Country Chart.

US sanctions and "Sensitive technology" provision

In addition to the US export control regime that is in place globally for all countries, the US government has imposed a number of sanctions against specific countries and actors. Currently, the US has comprehensive sanctions in place against five countries: Iran, Syria, Sudan, North Korea, and Cuba. These sanctions regulations are different from the global export control regulations. Yet, sanctions regulations are also a source of precedents for how to treat surveillance technology and provisions worth considering for the export control regime.

For example, beginning in 2010, the US government prohibited the export of goods or services that the government has designated as "sensitive technology"[50] to Iran through the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010. Sensitive technology is defined as hardware, software, telecommunications equipment or any other technology used specifically "1) to restrict the free flow of unbiased information in Iran; or 2) to disrupt, monitor or otherwise restrict speech of the people of Iran."[51] This provision was later expanded to include Syria through legislative and administrative actions such as the Iran Threat Reduction and Syria Human Rights Act of 2012, Executive Order 13606 (the GHRAVITY E.O.) and Executive Order 13628.[52] This sets precedents for controlling surveillance technology as part of the broader export control regime covering exports

Figure 3

Level of restrictiveness *low* ⟷ *high*		
Unrestricted EAR: §740.17(b)(3)(iii) ECCN: 5X002	Restricted EAR: §740.17(b)(2) ECCN: 5X002	Surreptitious Listening EAR: §742.13 ECCN: 5A001.i and 5X980
Forensic data capture and analysis for evidence or law enforcement use	Lawful intercept gateway (as designed for government) and cryptanalytic items	Surreptitious listening items that could be used for unlawful interception of wire, oral or electronic communications
BIS will review before export to government or non-government end users	BIS requires a license for government end users and will review before export to non-governmental end users	BIS requires license for all exports and destinations with a general policy of denial except for communications providers, U.S agencies, and related contractual parties
License exemption "Encryption commodities, software and technology" (ENC) available for both government and non-government end users after registration and classification	License exemption ENC available for both government and non-government end users after registration and classification	License exemption ENC not available
*Specific details and ECCNs available at: http://www.bis.doc.gov/index.php/licensing/commerce-control-list-classification/commerce-control-list-ccl/17-regulations/139-commerce-control-list-ccl		

generally.

Recent example of penalty due to export of Internet surveillance technology to Syria

The BIS's 2014 Report on Foreign Policy-Based Export Controls offers another example of the growing recognition generally by the government that the new surveillance market is a problem. The report specifically mentions a penalty resulting from an export of Internet surveillance software to Syria. It states that "on three occasions between October 2010 and May 2011, Computerlinks FZCO engaged in transactions or took actions with intent to evade the Export Administration Regulations in connection with the unlawful export and re-export to Syria of equipment and software designed for use in monitoring and controlling Web traffic".[53] The government invoked ECCN 5A002 and 5D002 referencing National Security, Anti-Terrorism, and Encryption Items. The penalty was $2,800,000 – twice the value of the export – and audit requirements.

This example, even though it focuses on a country subject to US sanctions, demonstrates that the government is generally becoming more aware how this new technology can be abused and the negative consequences of uncontrolled surveillance. It offers insight into how such technology can be regulated as part of the broader export control regime.

(2) UK EXPORT CONTROLS

The UK is the world's 11th largest exporter and fifth largest importer of merchandise.[54] It has also historically been one of the world's leading arms exporters; it was the sixth largest exporter of major conventional arms in terms of value for the period from 2008 to 2012,[55] and according to UK government figures, is the second biggest defense exporter in the world and the fifth largest exporter of security products.[56] The UK defense and security industry is consistently argued to be a key driver of growth and innovation in the country and a major provider of jobs and is heavily subsidized – it is estimated that in 2009/10 it was subsidized by nearly £700 million.[57] In regard to surveillance equipment, Privacy International has identified 77 UK-based companies exhibiting surveillance systems and technologies at trade shows across the world since 2009.[58]

The UK is currently in the midst of an effort to double its exports to £1 trillion by 2020 – a strategy focusing heavily on security exports and specifically "cyber security" exports. There has been an increasing emphasis on expanding such exports given the UK's relative strength in skills and research and within the defense and security sector. Defense and security exports from the UK amounted £11.5 billion in 2012, up from £8 billion in 2011. UK exports in the security sector grew 4% over the same period, to £2.7 billion.[59]

Problematically, within the scope of equipment identified in the UK's strategy for increasing cyber security exports is deep packet inspection equipment that can be used for censorship and surveillance while other law-enforcement technologies are apparently also being promoted by the UK government as part of its cyber security export strategy.[60]

General introduction to UK export controls

The UK's export control infrastructure has developed around the UK's high level of defense and security exports and is relatively robust in terms of legislation and enforcement; indeed there will be no need to enact any primary legislation to ensure that the UK's export control system is in line with principles underpinning the newly agreed Arms Trade Treaty – an initiative that the UK government was hugely influential in pushing forward at the United Nations.

Licensed exports of military and dual-use goods are considered on a case-by-case basis against eight criteria based on the EU Code of Conduct. Some surveillance equipment is currently explicitly subject to licensing and is therefore considered against these criteria. However, the majority of such equipment is either not explicitly controlled or controlled adequately.

Legislative framework for UK export controls and implementation

Statutory law concerning the UK export control system is derived from EU and UK national legislation. Primary UK legislation on export controls is defined within the 2002 Export Control Act and is subject to amendment by secondary legislation in the form of orders, the most notable one of which is the 2008 Export Control Order. While legislation is primarily based on parliamentary statutory law, the UK is also directly subject to superseding EU legislation. Through its export control system, the UK has also agreed to a range of UN Resolutions, treaties and international agreements concerning, for example, non-proliferation, arms control, sanctions, human rights, and chemical, biological, radiological, and nuclear explosive weapons.

The Consolidated List of Strategic Military and Dual-Use Items that require Export Authorization

(The Consolidated List) details what specific goods, technology and assistance are considered to be strategic exports and thereby subject to export controls for different strategic reasons. If an exporter wishes to export a product or service that falls within the consolidated list, they are required to apply for an export license. The application is subsequently reviewed on a case-by-case basis with regard to UK policy and a consolidated list of criteria for the export of military and dual-use goods, the Consolidated EU and National Arms Export Licensing Criteria (The Consolidated Criteria).

Overall responsibility for policy concerning export controls falls under the Department for Business, Innovation and Skills, while legislation is imposed by the Secretary of State for Business, Innovation and Skills under provisions of the Export Control Act 2002. The Export Control Organisation (ECO) is the specialized body within the department responsible for processing all license applications, for negotiating export control policy on the behalf of the UK, and for developing UK export licensing legislation with consultation from other departments. The Department for International Development, the Foreign and Commonwealth Office (FCO) and the Ministry of Defence (MoD) can be consulted within the license application assessment process, while the security services and GCHQ provide technical assistance and intelligence related to enforcement. Her Majesty's Revenue & Customs is the department that is responsible for the enforcement of export controls through the customs network and for investigating breaches of controls in coordination with the Crown Prosecution Service.

Exporters can apply for several different types of licenses. In general terms, the biggest distinction between them is the restrictiveness of what can be exported within a particular license; individual licenses typically allow an individual or company to export an expected amount of goods to a particular destination, while general licenses are less restrictive and can be used to authorise exports without explicit need for permission from the ECO for each export. There are also licenses for intra-community transfers within the EU and trade licenses for brokering and transit/transshipment. Items on the UK Military List requiring trade licenses are split into three categories according to the level of risk and the level of restrictions that apply; the trade in cluster munitions and torture equipment in Category A, for example, is more heavily regulated than less risky items in Category C.

The Consolidated List

Figure 4

Control List	Legislative Basis
UK Military List	Schedule 2 of the Export Control Order 2008
UK Dual-Use List	Schedule 3 of the Export Control Order 2008.
UK Radioactive Source List	Schedule referred to in Article 2 of the Export of Radioactive Sources (Control) Order 2006
UK Security and Human Rights List	Articles 9 and 4a of Export Control Order 2008
EU Human Rights List	Annexes II and III of Council Regulation (EC) No. 1236/2005 as amended by Regulation (EU) No 1352/2011
EU Dual-Use List	Annex 1 of Council Regulation (EC) No. 428/2009 (as last amended by Regulation (EU) No. 388/2012.

The Consolidated List is derived from national and international lists of controlled items as shown in Figure 4.

The Consolidated Criteria

The UK assesses applications for the export of items contained within the Consolidated List against the eight criteria outlined by the EU Code of Conduct. EU member states must also take into account their external relations and the national security of allied nations in their arms export policies. Criterion five of the UK Consolidated Criteria stipulates that "The potential effect of the proposed export on the UK's defence and security interests," or of "allies, EU Member States and other friendly countries" will be taken into account.[61] Article 10 within the Common Position also enables member states to take into full consideration the effect of an export on their national interests, as long as the other eight criteria are also taken into account. The UK Consolidated Criteria thus makes clear that the UK's economic, financial and commercial interests, its relationship with the recipient country and the effect of an export with regard to the protection of the UK's essential strategic industrial base will be considered in regard to any potential export.[62]

List-based Controls

The UK Military List is based on items that appear on the EU Common Military List and is used to define what equipment is covered by the EU Common Position. Changes to the Wassenaar Munitions List which were agreed upon in 2011 came into force in the UK on 20 March 2013.[63]

The EU Dual-Use list is identical to the items that appear within the annexes to the EU Dual-Use Regulation. Its legislative basis in the UK derives from Schedule 3 as referenced by Articles 2, 4, and 5 of the Export Control Order 2008. The UK also has unilateral controls on specific dual-use items within the UK Dual-Use List based on Article 8 within the EU Dual-Use Regulation and made in exercise of powers conferred in Section 3 of the Export Control Order.[64] The UK has made use of Article 8 for several types of goods, including 'Telecommunications and related technology' – which includes "tropospheric scatter communication equipment using analogue or digital modulation techniques for export to Iran".[65]

The EU Human Rights List in the UK is identical to the items that appear on the EU Torture Regulation.[66] As EU law, it is directly applicable in the UK. The UK Security and Human Rights List is a list of nationally controlled items based on Article 7 in the EU Torture Regulation that allows member states to impose their own national controls on a small set of specific equipment. Member states are required to inform the Commission if they make use of this article. The UK maintains a ban on the export of leg-irons, gang-chains and portable electric shock devices and a licensing requirement on other items under this provision. Its legislative basis in the UK derives from Article 9 of Export Control Order 2008.

In order to introduce these controls, the UK government decided to bypass the EU Commission and impose controls unilaterally by creating a new control list. The Export of Radioactive Sources Order was made in exercise of the powers conferred by sections 1, 5 and 7 of the Export Control Act 2002 and in accordance with paragraph 2(1) of the Schedule to the act.[67] This paragraph allows export controls to be imposed on any goods 'the exportation or use of which is capable of having a relevant consequence' related to:

- National security of the United Kingdom and other countries
- Regional stability and internal conflict
- Weapons of mass destruction
- Breaches of international law and human rights

- Terrorism and crime
- Objects of cultural interest[68]

The explanatory memorandum accompanying the 2006 Order explains that it was decided to impose unilateral controls as opposed to relying on action at European level and on the ability of UK industry to self-regulate in order to provide exporters with regulatory certainty and because of the fact that any European regulation would need to be transposed into UK legislation anyway.[69] A similar procedure to introduce unilaterally the items within the Radioactive Source List could also be used for surveillance technology.

"Catch-all" Controls

An export can be made subject to authorization and be prohibited because of the end-use of an item, even if it does not appear on the Consolidated List. End-use controls allow UK authorities to stop the export of military or dual-use goods if there is a risk that items will be used as part of a Weapons of Mass Destruction (WMD) program or be exported for military purposes to a destination under embargo. Such "catch-all" controls also allow UK authorities to prohibit the export of items not listed in the Consolidated List where they have informed the exporter that the potential export is of such a risk. Such proactive monitoring is conducted within the counter-proliferation and arms control divisions across various government bodies. The UK Restricted Enforcement Unit, for example, brings together the FCO, the MoD, GCHQ, MI5 and MI6 bi-weekly to review any intelligence related to such exports.

Existing UK export controls relating to surveillance technology

Some surveillance systems are directly controlled in the UK as a result of them being subject to specific EU Restrictive Measures or because they appear on the EU Dual-Use list. Although items that are used to identify mobile telecommunications details such as international mobile service identity (IMSI) numbers were added to the Wassenaar Dual-Use list in 2011, the slow rate at which the EU has taken to update its Dual-Use Regulation to reflect this means that these items are still not in the UK Consolidated List.

Items that fall under ML11, Electronic equipment (including equipment capable of signal collection from mobile phone systems), are only licensable if they are "specially designed or modified for military use". There is no formal understanding of what "specially designed for military use" means in the UK: officials within the export authority assess the original design intent of a product to determine whether it is specifically designed for military use. A written answer in 2011 regarding ML11 and the sale of surveillance technology by Creativity Software to repressive regimes from Parliamentary Under-Secretary for BIS, Baroness Wilcox, stated that exports were not specially designed for military use and not therefore subject to the controls of ML11.[70]

If an item is marketed at law enforcement agencies as well as the military, it will not be considered as specially designed for military use in the UK.[71] Some surveillance systems arguably fall within the scope of UK controls because of the encryption used within the product. For example, BIS stated in June 2012 that Gamma International needs an export license for its FinSpy product because of the encryption controls.

UK government's current position on export controls and surveillance technology

Surveillance equipment can be brought within the scope of UK export controls by either adding items to one of the preexisting lists within The Consolidated List, by adding a new list, through the use of "catch-all" controls, through the use of sanctions, or through the use of interim measures.

Adding items into preexisting lists can be done in a number of ways. The items contained within the UK Military List, the EU Dual-Use List and the EU Human Rights List are based on negotiations and decision-making processes within external forums such as the Wassenaar Arrangement. Agreement on inclusion of surveillance equipment at the European and Wassenaar Arrangement level will therefore be reflected within the UK's own list. National controls can also be imposed however, as long as it is consistent with EU law, proportionate to the desired outcome, does not impose unnecessary costs on legitimate trade, and is capable of being effectively enforced.[72]

After letters highlighting the issue by Privacy International and complaints made against Gamma International in addition to public debate, the UK Government publically declared its intention to pursue international agreement to expand the scope of export controls to include some types of surveillance equipment in 2013. William Hague, First Secretary of State and Secretary of State for Foreign & Commonwealth Affairs wrote a letter stating,

> Discussions involving both EU and non-EU partners on the subject of extending controls on the export of surveillance technology are ongoing within the Wassenaar Arrangement. The Government believes that the existence of software designed to penetrate the defences of computers and communications devices and to record, modify and/or relay data without the user's knowledge poses a threat to national security, industry, and commerce, as well as to human rights.[73]

These changes were ultimately adopted at the 2013 Wassenaar Arrangement plenary meeting.

The UK can exercise emergency powers to impose restrictions at short notice under the 2002 Export Control Act. Section 6 authorizes "the power to impose any controls if the control order which imposes them provides for its expiry no later than the period of 12 months beginning with the day on which it is made."[74] These powers have been used for human rights purposes, namely in 2010 to establish an Order[75] controlling the export of the lethal injection anaesthetic sodium thiopental to the United States. This followed pressure from UK campaign group Reprieve and BIS concluding that legitimate trade in the drug would not be affected by banning the export of the drug to the US.[76]

The UK government's current position is not to pursue unilateral restrictions because it considers them to be ineffective given that they "could be more easily circumvented given the likelihood that many of the companies which manufacture such equipment will have offices in other EU and third countries."[77] As this report shows there are strong arguments why unilateral controls should be considered and its focus on three countries aims to support a broader multilateral push to enhance the effectiveness of the controls.

(3) GERMANY'S EXPORT CONTROLS

German export controls have historically been very limited. Following a period of highly restrictive trade laws enforced by the occupying powers after the Second World War, the first German foreign trade law ("Aussenwirtschaftsgesetz" or AWG) of 1961 was the exact opposite, limiting regulation and enabling trade whenever possible.[78] Due to its liberal trade laws, Germany was held up as a less restrictive model to which the US should aspire after the end of the Cold War.[79] However German export law was tightened considerably after the Rabta and Samarra scandals in 1989/1990 where German companies were involved in the building of chemical weapons plants in Iraq and Libya.[80]

Legislative framework for Germany's export controls

German Foreign Trade Law – "Aussenwirtschaftsgesetz"

The key instrument is the Aussenwirtschaftsgesetz (AWG) and the associated administrative implementation agreement the Aussenwirtschaftsverordnung (AWV). Revised versions of both of were passed into law on September 1, 2013. In addition, a supplementary preamble was introduced by the left-wing SPD-Green governing coalition in the year 2000 and has been kept in force to this day. This preamble is designed as a 'political compass' to influence its interpretation and explicitly suggests that exports should be restricted to promote 'human rights'. While the preamble is designed to influence the interpretation of the law, it is not legally binding in a strict sense. As a result, scholars have argued for a legally binding interpretation of this preamble to be included within the legal provisions of the AWG.[81]

The AWG was recently extensively 'simplified' and many provisions were relaxed by the ruling conservative liberal CDU-FDP coalition in mid-2013 and reduced from 50 articles to 28. The changes to the law were justified by referring to EU-harmonization of export controls and a policy to promote exports (more details on the EU are outlined in the section specifically dedicated to the EU below).[82]

The AWV contains a long list of goods to be regulated including those set by international mechanisms such as the EU dual-use regulation and the Wassenaar dual-use regulations in addition to national controls. (REGULATION (EU) No 428/2009) and (REGULATION (EU) No 388/2012). As the German AWG and AWV existed before the EU dual-use regulation, German national laws needed to be updated in order to ensure they did not conflict with the EU dual-use regulations. Preventing this conflict is one important reason for the update of German dual-use regulations that came into force September 1, 2013.

There are two ways of changing the German AWV dual-use list: following §12(1) and §4(2) AWG small and mainly technical updates can be made directly by the German Federal Ministry of Economic Affairs in close coordination with the Federal Ministry of Foreign Affairs and the Federal Ministry of Finance. However, larger changes require the whole German cabinet to make such decisions if they related to German security interests, international peace and security, or might cause serious harm to German foreign relations, §12(1) and §4 (1) AWG.[83]

The new German legal framework of AWG and AVW also includes legal provisions regarding a national implementation of Article 4 and Article 8 of the EU dual-use (REGULATION (EU) No 428/2009). While §9 AWV includes provisions which implement Article 4 of the EU dual-use regulation,

we were not able to find any regulations for a German implementation of Article 8.

As far we are aware the right of the German government to restriction exports through Article 8 EU Dual-Use (REGULATION (EU) No 428/2009) due to either human rights or public safety concerns is not included in the German AVG or AVW. In order to use its right under Article 8 EU-Dual-Use VO to restrict exports due to human rights concerns - as the Italian government did when confronted with a public debate about Area Spa exports to Syria[84] – the German AVW would first need to be updated to include such provisions. While Germany has the right to use its Article 8 EU Dual-Use (REGULATION (EU) No 428/2009) powers, it is unlikely that it would do so without first defining what the process for the use of such powers is. These changes would need to be made at Cabinet level by the ruling German government.

Weapons Control Law – "Kriegswaffenkontrollgesetz" (KrWKG)

There is also a separate weapons control law 'Kriegswaffenkontrollgesetz' (KWKG) in Germany, which was passed in 1990. This law has an extremely narrow definition of weapons, only including goods whose only possible usage is for military purposes. As such, a tank may be listed among the restricted goods but its engine may not, if it can also be used in a tractor or as an industrial engine. As a result, even though politicians from all parties have called for surveillance technologies to be regulated, including one politician from the FDP suggesting they are added to the KWKG.[85]

Moreover it is important to note that the German Federal Police BKA have purchased a copy of FinFisher, as doing so essentially demonstrates obvious non-military uses from the perspective of the German state. Thus even Trojan horses like FinFisher cannot reasonably be argued to be single use 'weapons of war' in the German context, but would be considered dual use. There is, however, the separate category of Kriegsgeräte ('war goods'), such as night-vision goggles, which are part of the AWG and into which supporting technology and systems could fall. Finally, although the KWKG follows more restrictive principles than the AWG, the KWKG is embedded within the AWG. The KWKG covers only a very short list of items with a large part of the Wassenaar Agreement list instead embedded within the AWG under additional categories such as 'war goods' or just simply as dual-use items.[86]

Structure of Germany's export controls and implementation: The role of Executive and Parliament in changing the AWV

As stated above, modifications or changes to the AWV are made either by the German Federal Ministry of Economic Affairs in coordination with two other ministries or the whole cabinet. Consequently, the German Parliament has little control over the administrative implementation of the AWG. While the Parliament can express displeasure with the implementation of a law as regulated in a 'Verordnung' and the Bundesrat (upper house) has the right to comment, it does not have the power to change them. It can, however, change the law on which the 'Verordnung' is based on giving the executive the power to create a specific set of 'Verordnungen.' The German Federal Ministry of Economics and Technology (BMWI) is the main ministry administratively responsible for developing updates to the AWV list, typically in response to recommendations and expertise provided by the German Federal Office of Economics and Export Control (BAFA).

Implementation of the AWG

The way the AWG is implemented is designed to minimize burdens on exporters, putting the burden of proof on government agents. These agents are required to demonstrate concrete harms that are

likely as a result of the export, a potential threat of harm is not enough.[87]

Export licenses are provided by the Federal Office of Economics and Export Controls (BAFA or 'Bundesamt für Ausfuhrkontrolle') based in Bonn and generally take between 2 weeks and several months to be issued. The BAFA can issue individual export licenses, collective export licenses and single export licenses up to a certain financial transfer volume.[88] The applications are assessed against the criteria in the AWV and the EU Dual Use Regulation. BAFA also have some expertise in regulating technology and have done so in regards to software and computer systems in the past. BAFA Section 314 is responsible for regulating "Electronics, Telecommunications technologies and military electronics", while Section 212 "Authorization for Dual Use Items" is responsible for assessing applications. In the granting of these licenses, the BAFA frequently requests opinions from the BMWI and the German Ministry of Foreign Affairs (MFA).[89]

In such cases, both the BMWI and the German MFA have de facto veto rights, although the former typically promotes exports and the latter typically expresses concern. The responsible individuals within the German MFA are Section 4-B-3, Section 413 "Export controls on conventional war goods and dual use goods to the MENA region, Africa, Americas, the EU and NATO", and Section 414 "Export controls on conventional war goods and dual use goods to Asia and non-EU non-NATO Europe". There is no documented involvement of other agencies in this process. It is an open question if the German intelligence agency (BND) is also involved in the process, as their section TW is responsible for counter-proliferation.

The actual border control process is enacted by the German customs agency (Zoll) which is responsible for controlling exports. The German customs agency is part of the ministry of Finance and is primarily responsible for ensuring compliance with customs regulations, restricting import and export of certain physical goods, receiving duties for types of goods, anti-counterfeiting, etc. The Zoll has access to the European customs information database and must plausibly also be informed about current export lists by the German BAFA. However it is unclear how exactly this exchange of information takes place between BAFA and Zoll.

Other important aspects of German export controls

a) Penalties

The newly updated Export control regulations of the AWG considerably increase the penalties for violating export control regulations. According to §18(2) AWG exporters can face penalties of up to 5 years in prison for violating EU dual-use regulations. Such penalties are only applied however in areas such as Terrorism, nuclear weapons or war goods. Thus following §19 AVG the export of regulated surveillance exports in Germany can only be punished by a fine, as this would be considered a misdemeanor. As long as surveillance technologies are not categorized as war goods (which as noted above seems highly unlikely) an infringement of German dual-use regulations will remain a misdemeanor. Following AWG §19(6) and (4) such an infringement is punishable with fines up to EUR 500.000.

b) Export Guarantees

A dual-use export license is also a requirement for being able to access export guarantees provided by the German government to ensure that exporters get paid. Even in the unlikely situation that export controls have little or no effect on the actual transfer of goods, preventing taxpayer-funded guarantees to the exporters of surveillance tech is a valid goal in and of itself. It is also likely to deprive exporters of surveillance tech of an important

source of funding and increase the cost of doing business for surveillance vendors. Thus it can be argued that instituting licensing requirements for surveillance technologies have all manner of useful knock-on effects.

c) Regulating services, maintenance and technical support

One of the most interesting sections of German export control law pertains to the regulation of services, which are explicitly excluded in Article 7 of EU dual-use (REGULATION (EU) No 428/2009). As many of the surveillance tech services we noted in this report are systems that require a lot of maintenance and technical support, it would seem particularly appropriate to use this part of the regulation to 'catch' parts of the systems. Sadly such restrictions in the German AWV and AWG only apply to maintenance of nuclear plants and similarly heavily restricted systems. They do not currently apply to surveillance technologies.

d) Catch-all elements

The former as well as the newly updated export control regulations of the AWV contain a set of catchall elements (§§ 9 I, II, 11 I, III AWV). These apply to goods which are not covered by the export control list but might be used for either military or nuclear purposes, and are supposed to go to a recipient resident to a country specified in the provisions itself or in country list K. The transport of such goods within the EU, as well as the export into non-EU countries requires a permission of the Federal Office of Economics and Export Controls (BAFA).

Existing German export controls relating to surveillance technology

As in other EU countries, some surveillance systems are directly controlled in Germany as a result of them being subject to specific EU Restrictive Measures or because they appear on the EU Dual-Use list. Although items that are used to identify mobile telecommunications details such as IMSI numbers were added to the Wassenaar Dual-Use list in 2011, the slow rate at which the EU has taken to update its Dual-Use Regulation to reflect this means that these items are as of 2013 still not in the AWV List.

Items that fall under ML11, Electronic equipment (including equipment capable of signal collection from mobile phone systems) are included in the AWV List and fall under "Section A: List of weapons, ammunition and military equipment." As such they are only licensable if they are "specially designed or modified for military use." The export of surveillance technologies does not require an export license, unless they include cryptography. In such cases, the German government does limit the sale of technologies while also including certain types of cryptography in line with the Wassenaar arrangement. However very little information about such exports is available.

(4) EU EXPORT CONTROLS

Currently the 28 member states of the EU share a single external customs border and external trade policy and agreements are negotiated and decided at EU level. Trade with non-EU members, or third countries, is defined within the EU Common Commercial Policy and is an important area in which the EU practices competence over national governments. The creation of a single customs union across the European Union (EU) was also one of its central driving forces and remains one of the core areas of policy that is under the exclusive competency of the EU.

EU member states have also increasingly pursued efforts to harmonize defense and security export practices. There are several reasons for this:[90] The emergence of the Common Foreign and Security Policy (CFSP) and the European Security and Defense Policy (ESDP) beginning in the early 1990s provided a regulatory basis for such efforts, while major arms-exporting member states were also strongly incentivized to harmonize arms exports practices with the growth and internationalization of their defense and security sectors. The end of the Cold War also saw an increased emphasis on human rights and ethical practices related to arms exports, while at the same time the demonstrable ease with which national controls could be circumvented highlighted the need for a harmonized approach towards legislation and enforcement.

There have been increasing efforts to ensure that surveillance technology is not exported from Europe and used for internal repression or violations of human rights in the wake of the Arab Uprising. The EU today provides policy and legislates in several relevant areas, most notably in the areas of arms export controls, dual-use controls and sanctions policy. Other initiatives, such as the Torture Regulation, are also of comparative relevance.

Arms Export Controls

Commitments made by member states on arms exports at the EU level shape export control systems and strategic trade policies. Efforts aimed at harmonizing arms exports practices among member states began in the early 1990s with the creation of the Working Group on Conventional Arms Exports (COARM) and establishment of eight common criteria to be used in the assessment of arms export license applications.[91] The 1998 EU Code of Conduct expanded the criteria and committed member states to intelligence sharing and transparency measures.

Today, EU member states are politically obliged to implement legislation conforming to Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment (The Common Position). The Common Position was adopted in 2008 as a successor to the Code of Conduct and along with criteria for states to use when assessing arms exports, also commits them to exchanging intelligence on their arms exports – including cases where an application has been denied – and to exchanging information related to their export policy and practices. In addition to EU member states, Bosnia and Herzegovina, Canada, Croatia, the former Yugoslav Republic of Macedonia, Iceland, Montenegro, and Norway have aligned themselves with the criteria and principles of the Common Position.

The eight criteria (see: Figure 5), generally outline considerations related to human rights, the risk of diversion, economic development, and the threat to regional peace and security that should be considered when exporting controlled military items.

Figure 5

ONE	Respect for the international commitments of EU member states, in particular the sanctions decreed by the UN Security Council and those decreed by the Community, agreements on non-proliferation and other subjects, as well as other international obligations
TWO	The respect of human rights in the country of final destination
THREE	The internal situation in the country of final destination, as a function of the existence of tensions or armed conflicts
FOUR	Preservation of regional peace, security and stability
FIVE	The national security of the member states and of territories whose external relations are the responsibility of a Member State, as well as that of friendly and allied countries
SIX	The behaviour of the buyer country with regard to the international community, as regards in particular to its attitude to terrorism, the nature of its alliances and respect for international law
SEVEN	The existence of a risk that the equipment will be diverted within the buyer country or re-exported under undesirable conditions
EIGHT	The compatibility of the arms exports with the technical and economic capacity of the recipient country, taking into account the desirability that states should achieve their legitimate needs of security and defense with the least diversion for armaments of human and economic resources

Along with information sharing and cooperation measures between EU member states' export control authorities, the EU also publishes a Common Position User's Guide to direct policy and implementation of the criteria. With respect to Criteria Two, the User's Guide stipulates that:

> "Having assessed the recipient country's attitude towards relevant principles established by international human rights instruments, Member States shall:
>
> (a) deny an export licence if there is a clear risk that the military technology or equipment to be exported might be used for internal repression.
>
> (b) exercise special caution and vigilance in issuing licences, on a case-by-case basis and taking account of the nature of military technology or equipment, to countries where serious violations of human rights have been established by the competent bodies of the United Nations, by the European Union or by the Council of Europe;
>
> – Having assessed the recipient country's attitude towards relevant principles established by instruments of international humanitarian law, Member States shall:
>
> (c) deny an export licence if there is a clear risk that the military technology or equipment to be exported might be used in the commission of serious violations of international humanitarian law."

The inclusion of "clear risk" and "might" in this context is significant in that it requires a lower burden of evidence than if the export *will* be used for internal repression or in the commission of serious violations of international humanitarian law.[92]

In addition to common assessment criteria and cooperation, EU member states also share a common list of military items mirroring the

Wassenaar Munitions List against which the criteria are applied. The EU Common Military List itself has the status of a commitment in the framework of the Common Foreign and Security Policy[93] and is updated annually. The last update of the Wassenaar list agreed in 2011 was adopted in February 2012 by the Council and published as a Directive by the Commission in December 2012.

The military list applies to some surveillance technology where they have been designed for military use, including category ML11 (see below). Member states, such as the UK, can also use the criteria to assess exports of dual-use exports.

Dual-Use Controls

Council Regulation (EC) No 428/2009 (EC), the "Dual-Use Regulation", updated EU controls on dual-use items and seeks to harmonize export, intra-community transfer, brokering and transit procedures in regard to dual-use items across EU member states. The Dual-Use Regulation is currently undergoing a major review since a Green Paper on the EU dual-use export control system was published for public consultation in October 2011. The Directorate General for Trade oversees dual-Use controls within the European Commission, while the International Trade committee is responsible for dual-use policy in the Parliament.

The EU Dual-Use Regulation pulls in dual-use items that are agreed and included within the control lists of the Wassenaar Arrangement as well as those of the other multilateral regimes: the Missile Technology Control Regime, the Nuclear Suppliers' Group, the Australia Group and the Chemical Weapons Convention. Updates to the EU Dual-Use List to reflect changes to the multilateral export control regimes lists have been slow; a Council Regulation amending the EU dual-use list to reflect changes made to the multilateral control lists throughout 2010, for example, was only enacted across the EU in April 2012 by Regulation (EU) No 388/2012.[94]

Two main reasons have been cited for this delay: the first relates to the fact that the four multilateral control regimes meet and update their lists at different periods in the year. The second reason stems from the fact that the Lisbon Treaty gave the EU Parliament co-decision powers over any updates to the Dual-Use Regulation.[95] Commission Proposal 2011/0310 sought to minimize this delay by replacing the use of the ordinary legislative procedure for updating the Dual-Use Regulation with delegated acts, which would allow the Commission to unilaterally make updates.

As part of the Parliament's co-decision powers over any such changes, Parliamentarians endorsed in October 2012 amendments to the proposal tabled by Dutch MEP and long-time advocate of stronger regulation in the area, Marietje Schaake (D66/ALDE). The amendments would have placed an authorization requirement on exporters if they have been informed that the transfers of surveillance technology "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".[96]

The Commission did not accept the amendments, however,[97] and the proposal is still making its way through the law-making process between the Parliament and the Commission and awaiting first reading at the Council. The issue is not expected to be resolved until summer 2014.[98]

In addition to providing a common Dual-Use list for EU member states, the Dual-Use Regulation also introduced Community General Export Authorisations (GEAs) – EU-wide licenses aimed at streamlining the export of specific items to specific destinations. There are currently six categories of goods, including category EU005 on

Telecommunications. European Parliamentarians reached a decision with the Council that prohibited the export of Surveillance technology with EU GEAs where there are human rights concerns.[99] Under the 2011 Regulation 1232/2011, items were made ineligible for use under a GEA if they were to be used:

> "...in connection with a violation of human rights, democratic principles or freedom of speech as defined by 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 (e.g. via Monitoring Centers and Lawful Interception Gateways)."[100]

EU Restrictive Measures

Surveillance and monitoring equipment has been adopted within embargoes as part of sanctions regimes at the European level. EU Restrictive Measures can be imposed within the framework of the Common Foreign and Security Policy (CFSP) and as EU Regulations, making them directly applicable across all member states. As a CFSP instrument however, any Council Decisions require unanimity from member states in the Council.[101] Regulations can also be implemented with national legislation in member states to make provision for enforcement activities.[102]

The EU has so far included surveillance and monitoring equipment on Restrictive Measures targeting Syria and Iran. Following a Council Decision in December 2011, Council Regulation (EU) 36/2012 in January 2012 imposed a ban on the sale, supply, transfer or export, directly or indirectly of surveillance equipment, technology or software "whether or not originating in the Union, to any person, entity or body in Syria or for use in Syria."[103] A list of items was included within Annex V to the Regulation. Similar measures were imposed within Council Regulation (EU) No 264/2012 targeting Iran in March 2012 and a list of items included within Annex IV to that Regulation.[104] While the binding nature of Restrictive Measures and the scope of equipment targeted is an encouraging development at EU level, there has been no publically available evidence to indicate the efficacy of these measures.

The fact that surveillance technology has only been included in the regimes targeting Iran and Syria and not across all restrictive measures is problematic. EU embargoes on equipment that might be used for internal repression – a category in which surveillance technology could fall but that currently does not – have however been adopted more widely, and it is appropriate that this list be expanded to include surveillance technology. In addition to the restrictive Measures in force targeting Iran and Syria, the export of equipment that might be used for internal repression has been banned as part of measures targeting Belarus, Cote d'Ivoire, Republic of Guinea, Libya, Myanmar (Burma), and Zimbabwe.[105]

Torture Regulation

Regulation No. 1236/2005, the "EU Torture Regulation", concerns restrictions on the trade in certain goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment.[106] The Torture Regulation was imposed pursuant to Article 6 of the Treaty on European Union concerning respect for human rights and fundamental freedoms and as EU law is directly applicable across member states. The Torture Regulation requires that the list of items to be controlled be kept under review; it was last amended by Commission Implementing Regulation No. 1352/2011 of 20 December 2011 in order to widen the scope of drugs used in lethal

injection. While it is a highly notable development in EU trade policy and in many respects offers a useful comparative example of how certain items detrimental to human rights can be effectively regulated, surveillance technology does not readily fall within the scope of equipment that is controlled under the regulation.

Catch-all Controls

Catch-all clauses allow national authorities to make items not listed within controls subject to authorization and are applicable to dual-use goods. The Wassenaar Arrangement stipulates that:

> "Participating States will take appropriate measures to ensure that their regulations require authorisation for the transfer of non-listed dual-use items to destinations subject to [an] arms embargo … when the authorities of the exporting country inform the exporter that the items in question are or may be intended, entirely or in part, for a military end-use."[107]

The EU Dual-Use Regulation also has provisions for catch-all controls. Article 4 of Council Regulation (EC) 428/2009 authorizes member states to make unlisted items subject to licensing if an item is used for a WMD program or a military end-use in a destination under a EU, OSCE, or UN arms embargo.[108]

However, "military end-use" refers to items that are incorporated into other items that already appear on the national military lists. The UK argues that this definition of military end-use is too narrow. For example, in its response to the EU Green Paper on EU dual-use export controls, the UK authorities stated that "we could prevent the export of an unlisted item intended to be used as a component in a military vehicle but we could not prevent the export of a complete civilian vehicle that was to be used by the military or internal security forces of the destination country even where that country is subject to arms embargo."[109] The UK proposes to redefine military end-use to mean "Intended for military, paramilitary, security or police forces in a destination subject to an arms embargo or to an entity involved in procurement, manufacture, maintenance, repair or operation on their behalf."[110] As of 2013, progress on this is developing as part of the EU dual-use controls review process.

Article 8 of the Dual-Use Regulation allows the extension of controls to non-listed items for reasons of public security or because of human rights considerations.[111] Member states are required to inform the Commission if they make use of this article. The UK has made use of this article for several types of goods, including tropospheric scatter communication equipment using analogue or digital modulation techniques for export to Iran.[112] In 2012, Italy used Article 8 to impose an authorization requirement on the export of a "Public LAN database centralised monitoring system" to the Syrian Telecommunications Establishment. [113] The move was in reaction to reports by Bloomberg[114] detailing how Italian firm Area SpA was installing a monitoring centre in the country and came after strong civil society pressure from Privacy International, Human Rights Watch and Access, among others.

(5) THE WASSENAAR ARRANGEMENT

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a multilateral export control regime. It consists of 41 participating states including the US, Russia, all EU member states (except Cyprus), Turkey, Canada, Mexico, Argentina, South Africa, Japan, and South Korea among others. They decide what items should be subjected to their national export controls for reasons of international security and stability. Inclusion of items within the Wassenaar Arrangement's control lists means that they become subjected to national export controls and to measures aimed at promoting transparency and harmonizing policies and practices.

History & Purpose

The Wassenaar Arrangement was formally established in 1996 as a successor to the Cold War Coordinating Committee for Multilateral Export Controls (CoCom) - a forum used by Western-bloc states to regulate arms exports to Eastern-bloc states. Since its formation, the Wassenaar Arrangement's membership has grown to 41 participating states – including Russia – and includes eight of the world's top 10 exporters of major conventional weaponry, together accounting for some 80% of such exports.[115] While China and Israel are not participating states (and are important exporters of surveillance technology), Israel bases its export controls on the Wassenaar Arrangement's control lists and China's conventional weaponry control lists parallel those of the Wassenaar Arrangement. Further, many non-participating states also base their control lists on the Wassenaar Arrangement, further reinforcing its role as a norm-making and standard setting forum for transfers of conventional arms and dual-use goods.

A major difference from CoCom is the fact that the Wassenaar Arrangement is not directed at any states in particular; it instead seeks to harmonize export systems and policy among participating states. Its stated aim is to "contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods, thus preventing destabilizing accumulations." As a forum focusing on "destabilizing accumulations," human rights or internal repression issues are not explicitly considered. Implementation is left to the discretion of national states, in line with their national policies and legislation, although principles for objective analysis of license applications are provided.

Function

The Wassenaar Arrangement contains two control lists: a List of Dual Use Goods and Technologies, and a Munitions List. The Munitions List contains conventional arms such as armed combat vehicles and small arms, while the Dual-Use list contains items that have both a civilian and military application such as navigation equipment and certain avionics. Some categories of items are also included in a 'Sensitive' and 'Very Sensitive' list, meaning that their trade is subject to greater scrutiny and intelligence-exchange measures among states. In addition to the control lists, states also agree on best practices and transparency initiatives with the aim of harmonizing policies and practices.

Each year, member states discuss including new items or updates to an existing item. These decisions are reached by consensus and in private among national authorities of participating states. Proposals to include new categories to the control list are initiated by participating states and

negotiated through various working groups focusing on technical and policy-related aspects. A plenary meeting, usually held in December, is the official decision-making and political body of the Arrangement that formally agrees on the new controls. The Arrangement is also supported by a small secretariat based in Vienna, Austria.

When considering whether to introduce new items into a control list, four criteria are considered:[116]

- The foreign availability outside of participating states;
- The ability to effectively control the export of the goods;
- The ability to make a clear and objective specification of the item;
- If the item is already controlled by another regime, such as the Australia Group, Nuclear Suppliers Group, or Missile Technology Control Regime.

Existing Controls of Surveillance Technology

While human rights and internal repression considerations are not the focus of the Wassenaar Arrangement, there are several existing categories within the Wassenaar Arrangement control lists that apply to surveillance technology. Such technology can significantly increase the military capabilities of a state, its ability to conduct espionage, and in some cases its ability to target foreign citizens, putting this technology within the scope of the Wassenaar Arrangement. A category targeting mobile telecommunications jamming equipment was introduced in 2010 and expanded to include interception and passive counter-surveillance equipment in 2012. In 2013, updates were agreed to the Dual-Use list to explicitly include malware-based surveillance products and IP network monitoring systems.

Within the munitions list, Category ML11 applies to "Electronic equipment specially designed for military use", including "Electronic systems or equipment, designed either for surveillance and monitoring of the electro- magnetic spectrum for military intelligence or security purposes or for counteracting such surveillance and monitoring". While this category could include many types of surveillance technologies, the stipulation that the item needs to be "specially designed for military use" greatly narrows the scope of this control.

Categories 5A002 and 5D002 within the Wassenaar Arrangement Dual-Use list are aimed at items that employ cryptography and therefore have been used to catch some surveillance technologies such as FinFisher. The export control of cryptographic items was a controversial policy response to security challenges in the 1990s and remains ineffective. As a key security measure to protect the confidentiality of communications and to ensure trust and confidence in digital interactions, encryption is an inappropriate control through which to catch surveillance technologies. Further, because of the indirect method through which it controls surveillance systems there remains the possibility that manufacturers can circumvent it by simply adjusting specifications within their products such as the key size or removing encryption from the product altogether. Last but not least, encryption controls need and are likely to be further liberalized in the future while export controls for surveillance technology must be updated and tightened.

The category within the 2012 Wassenaar Arrangement Dual-Use list that applies explicitly to surveillance technologies, namely IMSI catchers, is written as follows:

5. A. 1. f. Mobile telecommunications interception or jamming equipment, and monitoring equipment therefor, as follows, and specially designed components therefor:

1. Interception equipment designed for the extraction of voice or data, transmitted over the air interface;

2. Interception equipment not specified in 5.A.1.f.1., designed for the extraction of client device or subscriber identifiers (e.g., IMSI, TIMSI or IMEI), signalling, or other metadata transmitted over the air interface;

3. Jamming equipment specially designed or modified to intentionally and selectively interfere with, deny, inhibit, degrade or seduce mobile telecommunication services and performing any of the following:

   a. Simulate the functions of Radio Access Network (RAN) equipment;

   b. Detect and exploit specific characteristics of the mobile telecommunications protocol employed (e.g., GSM); or

   c. Exploit specific characteristics of the mobile telecommunications protocol employed (e.g., GSM);

4. RF monitoring equipment designed or modified to identify the operation of items specified in 5.A.1.f.1., 5.A.1.f.2. or 5.A.1.f.3.;

   Note 5.A.1.f.1. and 5.A.1.f.2. do not apply to any of the following:

   a. Equipment specially designed for the interception of analogue Private Mobile Radio (PMR), IEEE 802.11 WLAN;

   b. Equipment designed for mobile telecommunications network operators; or

   c. Equipment designed for the "development" or "production" of mobile telecommunications equipment or systems.

ANALYSIS OF 2013 WASSENAAR ARRANGEMENT CHANGES

In December 2013, the 41 member states of the Wassenaar Arrangement announced new controls relating to "intrusion software" and "IP network surveillance systems" arguing that they can be detrimental to international and regional security and stability. These two changes are apparently the result of two separate proposals from the French and UK governments. Once changes have been agreed upon through the multilateral Wassenaar regime, each member state is expected to integrate and implement the changes in its national export control regime which takes from a few months in some countries to two to three years in others.

1. "Intrusion Software"

The UK proposal was initially framed to focus on "Advanced Persistent Threat Software and related equipment (offensive cyber tools)."[117] The language adopted through the plenary of the Wassenaar Arrangement in December 2013 refers to "intrusion software". It is important to note that the definition of intrusion software is not a control itself. The actual controls to be regulated are stated later in reference to the definition. This difference is crucial because the language differentiates between the agent - "intrusion software" - and the infrastructure behind the agent. The term used, "intrusion software," is defined as:

> "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.

This section captures two key components of commercial malware such as systems sold by FinFisher. The first part covers the exfiltration of data from the victim's system such as microphone or camera streams. It also includes software that changes files on the victim's machine such as planting or altering images or video already on the victim's machine. The second component defines the mechanism by which commercial malware typically infects its victim's devices. Specifically, this is the exploit mechanism that the surveillance product takes advantage of. It achieves this by exploiting a vulnerability, a flaw whether disclosed or not, in a victim's system. There is no requirement for software to perform both A and B, it is sufficient for only one to be performed.

This language echoes the "offensive IT intrusion" marketing lines used by FinFisher[118] and others. It is focused on the fact that the targeted items are designed to avoid security features on a device. This feature is essential for many IT intrusion solutions being sold to governments. Brochures for Hacking Team's Remote Control System, for example, explain how it "bypasses protection systems such as antivirus antispyware and personal firewalls."[119] Similary, FinFisher boasts its capabilities provide for the "bypassing of 40 regularly test antivirus systems."[120]

Controlled Intrusion Software Infrastructure

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".

Intrusion software itself is therefore not controlled. Otherwise, a targeted user, whose laptop was infected with malware through a malicious email attachment, could be violating export controls when traveling to another country with the infected laptop. Instead, the wording of the controls is very explicit in that only components for the generation, operation, delivery and communication with the malware are subject to the control.

Intrusion technology is typically delivered as a software and hardware package. The customer receives a physical package that requires as little configuration as possible. Within very little time it can inject malicious software to exfiltrate keylogs, passwords, screenshots, microphone recordings, camera snapshots, Skype chats, and remotely execute nearly any command the intruder desires. Importantly, the new controls appear to specifically describe the components that stay under direct control of the purchaser, not any component that would end up on a victim's end-user device. In this manner, the control list targets those who purchase intrusion software and seek to target others, not those who are infected with it.

This command and control component is a crucial component of the surveillance packages that commercial malware vendors sell. The restrictions that malware vendors place on the further dissemination of their command and control

infrastructure and the lack of availability of the software to the general public appear to be decisive factors in determining whether this type of software is subject to the new controls. And these components all benefit from the general software exemption if it applies. Crucially, software to achieve these activities resides off the victim's device, while the intrusion software itself must reside on the device.

2. "IP network surveillance systems"

"IP network surveillance systems" aim at general traffic analysis systems such as deep packet inspection items, which can classify and collect information flowing through a network. The Internet Protocol (IP) is one of the core standards upon which today's communications infrastructure is built, enabling online searches, emails and VoIP calls among others. The interception of these communications lies at the heart of many mass surveillance systems. The French proposal seeks to control some of this technology and was 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):
>
> a. Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));
>
> b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and
>
> c. Indexing of extracted data; and
>
> 2. Being specially designed to carry out all of the following:
>
> a. Execution of searches on the basis of 'hard selectors'; and
>
> b. Mapping of the relational network of an individual or of a group of people.

This set of controls is targeted at a very narrow class of products with the various elements all being connected through "and" rather than "or" relationships. It therefore risks failing to adequately cover some of the systems that are of greatest concern. Additional noteworthy elements are:

- The controls call for the product to be "specially designed" to search through the captured data based on certain characteristics of an individual (such as name, political affiliation, tribe etc.). This data must be used to deliver what's known in the industry as "actionable intelligence," meaning it has to be able to collate the captured data to identify relationships between the targeted individual or group.

- What constitutes "carrier class" will be open to interpretation by member states, given that there are a number of definitions that could be cited by any of the competent bodies.[121]

- "Analysis at the application layer" significantly limits the scope of the control, given that many surveillance products operate at layers other than the application layer, which usually refers to applications such as Instant Message Access Protocol and BitTorrent among many others.

- Extraction of selected data and its indexing means that the product needs to be actively retrieving the metadata and content from the IP traffic as well as actively storing this data.

Avoiding New Crypto Wars

Export controls have a bad reputation in many technology circles, and for good reason. The "Crypto Wars" mentioned above were about loosening the encryption controls regulating how people could buy, sell and use cryptography that prevented people from being able to employ encryption techniques and technologies to protect their information and communications. While the controls were eventually changed, the Crypto Wars have shaped how many software engineers and open source advocates view export controls. For those in the arms control world however, export controls are considered a useful tool in constraining the general inclination of governments and defense manufacturers to sell weapons and other technology for national interest and profit.

The Crypto Wars offer useful lessons learned regarding the risk that export controls represent to the development and exchange of free and open source software. It is clear that such controls need to be carefully crafted, clear, with a process in place to clarify and provide additional information on implementation and interpretation. This will without doubt be one of the greatest concerns among many when it comes to subjecting surveillance systems to export control.

The Wassenaar Arrangement offers some best practices concerning the need to control the exchange of software dating as far back as 2006.[122] Importantly, open-source and free software is generally exempt from control under the Wassenaar Arrangement. The General Software Note[123] outlines that the Wassenaar Arrangement control lists do not control "software" which is any of the following:

1. Generally available to the public by being:

a. Sold from stock at retail selling points without restriction, by means of:

1. Over-the-counter transactions;

2. Mail order transactions;

3. Electronic transactions; or

4. Telephone call transactions; and

b. Designed for installation by the user without further substantial support by the supplier;

2. "In the public domain"[124]; or

3. The minimum necessary "object code" for the installation, operation, maintenance (checking) or repair of those items whose export has been authorised.

It is important to note that (1.) and (3.) do not release software that includes cryptography and is subject to the controls of Category 5 Part 2 of the Wassenaar Arrangement on "Information Security". Within the specific section on "information security" within the Wassenaar Dual-Use List however, they are released from control if they are made generally available to the public, subject to several other conditions. Cryptographic software that is in the public domain such as open-source software is therefore exempt from control.

The Wassenaar *Definitions of Terms Used in these Lists* outlines that "in the public domain" "means 'technology' or 'software' which has been made available without restrictions upon its further dissemination" differing from the American copyright notion of "public domain." It also includes the important note that "Copyright restrictions do not remove 'technology' or 'software' from being 'in the public domain'" considering that open-source software is distributed under copyright.[125] Last but not least, the General Technology Note also outlines the exceptions that controls do not apply to "technology"[126] "in the public domain,"[127] to "basic

scientific research"[128] or to the minimum necessary information for patent applications.

CONCLUSION

This paper provides an overview of the export control regimes of three key exporting countries: the UK, the US and Germany, as well as the Wassenaar Arrangement and export regulations within the EU. It looks closely at how surveillance technologies are currently subjected to licensing restrictions and explores avenues through which some of these technologies can be controlled.

Export controls can be an effective tool for protecting victims against abuses of surveillance technology. Updating the export control regulations is the essential first step to achieving this. At the same time, there is a risk that they are overly broad which needs to be addressed. A sound implementation policy including well-defined assessment criteria, reporting requirements, and enforcement are also required in each individual state and multilaterally to increase the effectiveness of the regime overall. It should be noted that new export controls were already created, and as a result it makes sense for civil society to engage constructively in their formulation.

In this context the recent amendments to the Wassenaar Arrangement are a step in the right direction. The current language supports a control of the infrastructure for intrusion software, not of intrusion software itself or vulnerabilities. The language of the control is very narrow because the language is not intended to affect vulnerability research. It is critical that the intent of the language remains intact as the new control is being implemented in the 41 member states.

Moreover, the information security provisions of the Wassenaar Arrangement are of concern and too strict. This is particularly important, as strong encryption is one of the few tools at the disposal of individuals to protect themselves against surveillance. By limiting the access of individuals to strong cryptography, the Wassenaar arrangement contributes to limiting their agency and thus has a negative effect on their right to privacy. These provisions must also be updated.

There has been much apprehension in technology circles after the Crypto Wars about the regulation of technology exports. A similar level of apprehension followed the disclosures by Edward Snowden regarding the question whether states can be considered trustworthy actors. This report does not argue for blind trust in the state to regulate the trade in surveillance technologies, but considers engagement to be critical to serve as a safeguard and to inform the policy process.

The wider security research sector should engage in the development of export controls. Not only will this provide greater clarity, it will also ensure that less-scrupulous actors do not harm the reputation and practices of the rest of the industry as a whole.

Civil society should continue to inform this process to ensure that some of the most intrusive technologies are not sold to some of the worst human rights abusers. Civil society can also contribute to provide a level of public scrutiny and accountability over both governments and companies in terms of their policies and practices.

States should update their export control regulations vis-à-vis surveillance technologies which will allow them to meet their human rights obligations and foreign policy objectives.

In this context, updating export control regulations can contribute to limiting the harm caused by these products. Export controls represent an opportunity for states to step up to the plate and take their international human rights obligations seriously. There are legitimate concerns about the potential unintended negative effects of the new Wassenaar controls that need to be taken seriously. That is

why it will be necessary to continue to monitor the process to ensure that states live up to their obligations, while also ensuring that states do not create controls that are overly broad.

It is clear that the proliferation of surveillance technology is a new problem that needs to be urgently addressed. Export controls are one piece of a broader policy framework to ensure that such technology will not be abused. They need to be updated and this paper provides an outline of precedents and recommendations to inform this process. Every day that goes by without improving the status quo, is a day when the rights of people around the world will be violated.

Endnotes

[1] Valentino-Devries, Jennifer, Julia Angwin and Steve Stecklow. 2011. "Document Trove Exposes Surveillance Methods." *The Wall Street Journal,* November 19. http://online.wsj.com/news/articles/SB10001424052970203611404577044192607407780?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052970203611404577044192607407780.html.

[2] Examples for this broader trend of commercialization are In-Q-Tel established in 1999 is a venture capital firm financed by the C.I.A. and Palantir, one of In-Q-Tel's beneficiaries boasting 1,200 employees today. See: Dealbook. 2006. "C.I.A.-Backed Venture Firm In-Q-Tel Loses Chief Executive. *Dealbook,* April 24. http://dealbook.nytimes.com/2006/04/24/cia-backed-venture-firm-in-q-tel-loses-chief-executive/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1.

[3] Cohn, Cindy. 2014. "Maryland Court Dismisses Landmark Case That Sought to Hold Cisco Responsible for Violating Human Rights." Last modified February 27. https://www.eff.org/deeplinks/2014/02/maryland-court-dismisses-landmark-case-sought-hold-cisco-responsible-violating/.

[4] Bureau of Industry and Security, US Department of Commerce. 2014. *2014 Report on Foreign Policy-Based Export Controls.* Bureau of Industry and Security.

[5] Gallagher, Ryan. 2012. "French Company That Sold Spy Tech to Libya Faces Judicial Inquiry Amid New Allegations." *Slate,* June 19. http://www.slate.com/blogs/future_tense/2012/06/19/amesys_facing_inquiry_in_france_over_selling_eagle_surveillance_technology_to_qaddafi_.html.

[6] Citizen Lab. 2014. "Tag Archives: Blue Coat." *Citizen Lab,* March 10. https://citizenlab.org/tag/blue-coat/.

[7] The Wall Street Journal. 2012. "The Surveillance Catalog." *The Wall Street Journal,* February 7. http://projects.wsj.com/surveillance-catalog/#/.

[8] Cohn, Cindy. 2013. "EFF Supports Human Rights Case Against Cisco for Selling Surveillance Technologies to China." *EFF,* August 15. https://www.eff.org/deeplinks/2013/08/eff-supports-human-rights-case.

[9] FIDH. 2013. "Amesys Case: The Investigation Chamber green lights the investigative proceedings on the sale of surveillance equipment by Amesys to Khadafi regime." *FDIH,* January 15. http://www.fidh.org/en/north-africa-middle-east/libya/Amesys-Case-The-Investigation-12752.

[10] Privacy International. 2013. "Privacy International, HMRC to go to trial over agency's refusal to reveal state of any investigation into Gamma International." *Privacy International* June 27. https://www.privacyinternational.org/press-releases/privacy-international-hmrc-to-go-to-trial-over-agencys-refusal-to-reveal-state-of-any.

[11] *Du Daobin, et al. v. Cisco Systems, Inc., et al.,* Federal District Court of Maryland (2014). https://s.eff.org/files/2014/02/24/4995755-0-12686.pdf.

[12] Crime Control and Detection. EAR §742.7. http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=45e6c763621277af6b2e198439bf50fe&r=PART&n=15y2.1.3.4.26#15:2.1.3.4.26.0.1.7..

[13] The World Trade Organization. "Trade Profiles: Germany, United Kingdom, United States." Last modified September. http://stat.wto.org/CountryProfile/WSDBCountryPFView.aspx?Language=E&Country=US,GB,DE.

[14] Stockholm International Peace Research Institute. 2013. *SIPRI Yearbook 2013: Armaments, Disarmament and International Security.* 10. Oxford: Oxford University Press.

[15] Bureau of Industry and Security, US Department of Commerce. 2013. *Annual Report to the Congress for Fiscal Year 2013.* 9. Bureau of Industry and Security.

[16] US Constitution. Article I. Section 8.

[17] Gates, Robert M. "Business Executives for National Security (Export Control Reform)." Speech, Washington, DC, April 20, 2010. Defense.gov. http://www.defense.gov/speeches/speech.aspx?speechid=1453.

[18] US Government Accountability Office. "Export Controls: Observations on Selected Countries' Systems and Proposed Treaties." Last modified June 28. http://www.gao.gov/products/GAO-10-557.

[19] Bureau of Industry and Security, US Department of Commerce. 2012. "BIS Technical Advisory Committees (TAC) Meeting Schedule." Last modified January 17. http://tac.bis.doc.gov/.

[20] For more specific details including dates of acts see: Fergusson, Ian F. and Paul K. Kerr. 2014. *The US Export Control System and the President's Reform Initiative.* CRS Report R41819. Appendix A. Washington, DC: Library of Congress, Congressional Research Service. https://www.fas.org/sgp/crs/natsec/R41916.pdf.

[21] Fergusson, Ian F. and Paul K. Kerr. 2014. *The US Export Control System and the President's Reform Initiative.* CRS Report R41819. Washington, DC: Library of Congress, Congressional Research Service. https://www.fas.org/sgp/crs/natsec/R41916.pdf.

[22] Fergusson, Ian F. and Paul K. Kerr. 2014. *The US Export Control System and the President's Reform Initiative.* CRS Report R41819. Washington, DC: Library of Congress, Congressional Research Service. https://www.fas.org/sgp/crs/natsec/R41916.pdf.

[23] Bureau of Industry and Security, US Department of Commerce. 2013. *Annual Report to the Congress for Fiscal Year 2013.* 8. Bureau of Industry and Security.

[24] Bureau of Industry and Security, US Department of Commerce. "Deemed Exports." Accessed March 20, 2014. https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports.

[25] Fergusson, Ian F. and Paul K. Kerr. 2014. *The US Export Control System and the President's Reform Initiative.* CRS Report R41819. Washington, DC: Library of Congress, Congressional Research Service. https://www.fas.org/sgp/crs/natsec/R41916.pdf.

[26] Bureau of Industry and Security, US Department of Commerce. 2014. "Commerce Control List (CCL)." Accessed March 18. https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl.

[27] Bureau of Industry and Security, US Department of Commerce. 2013. *Know the Facts Before You Ship: A Guide to Export Licensing Requirements*. Bureau of Industry and Security. http://business.usa.gov/external-site?ccontent=http://www.bis.doc.gov/index.php/forms-documents/doc_view/286-licensing-faq.

[28] US Department of State. 2014. "Overview of US Export Control System." Accessed March 18. http://www.state.gov/strategictrade/overview/.

[29] Bureau of Industry and Security, US Department of Commerce. 2013. *Commerce Control List Overview and the Country Chart*. Last modified

October 15. Bureau of Industry and Security. http://www.bis.doc.gov/index.php/forms-documents/doc_download/742-738.

[30] Bureau of Industry and Security, US Department of Commerce. 2012. *Commerce Control List Overview and the Country Chart*. Last modified July 23. Bureau of Industry and Security. http://www.bis.doc.gov/index.php/forms-documents/doc_view/14-commerce-country-chart.

[31] The White House Office of the Press Secretary. 2013. "Fact Sheet: Announcing the revised US Export Control System." Last modified October 15. http://www.whitehouse.gov/the-press-office/2013/10/15/fact-sheet-announcing-revised-us-export-control-system.

[32] The White House Office of the Press Secretary. 2010. "Fact Sheet on the President's Export Control Reform Initiative." Last modified April 20. http://www.whitehouse.gov/the-press-office/fact-sheet-presidents-export-control-reform-initiative.

President's Export Control Reform Initiative "From the ECR blog" available at http://export.gov/ecr/.

[33] Fergusson, Ian F. and Paul K. Kerr. 2014. *The US Export Control System and the President's Reform Initiative.* CRS Report R41819. Washington, DC: Library of Congress, Congressional Research Service. https://www.fas.org/sgp/crs/natsec/R41916.pdf.

[34] President's Export Control Reform Initiative "Export Control Reform News - February 4, 2013 " available at http://export.gov/ecr/eg_main_043652.asp

[35] Fergusson, Ian F. and Paul K. Kerr. 2014. *The US Export Control System and the President's Reform Initiative.* CRS Report R41819. Washington, DC: Library of Congress, Congressional Research Service. https://www.fas.org/sgp/crs/natsec/R41916.pdf.

[36] Center for Human Rights, American Bar Association American Bar Association. 2013. *White Paper: Proposals to Relax Export Controls for Significant Military Equipment.* American Bar Association. http://www.americanbar.org/content/dam/aba/administrative/individual_rights/jdweb_aba_chr_white_paper_on_proposals_to_relax_export_controls_for_significant_military_equipment_final.authcheckdam.pdf.

Hartung, William D. 2013. "Risks of Loosening Arms Export Controls Far Outweigh Benefits." *Open Society Foundations,* August 21. http://www.opensocietyfoundations.org/voices/risks-loosening-arms-export-controls-far-outweigh-benefits.

Fergusson, Ian F. and Paul K. Kerr. 2014. *The US Export Control System and the President's Reform Initiative.* CRS Report R41819. 21. Washington, DC: Library of Congress, Congressional Research Service. https://www.fas.org/sgp/crs/natsec/R41916.pdf.

[38] Fergusson, Ian F. and Paul K. Kerr. 2014. *The US Export Control System and the President's Reform Initiative.* CRS Report R41819. Washington, DC: Library of Congress, Congressional Research Service. https://www.fas.org/sgp/crs/natsec/R41916.pdf.

[39] *Du Daobin, et al. v. Cisco Systems, Inc., et al.,* Federal District Court of Maryland (2014). https://s.eff.org/files/2014/02/24/4995755-0-12686.pdf.

[40] Bureau of Indusrty and Security, US Department of Commerce. 2014. *2014 Report on Foreign Policy-Based Export* Controls. Bureau of Industry and Security. http://www.bis.doc.gov/index.php/forms-documents/doc_download/870-bis-foreign-policy-report-2014.

A special provision is in place for China as BIS's 2014 Report on Foreign Policy-Based Export Controls outlines: "Following the 1989 military assault on demonstrators by the PRC government in Tiananmen Square, the US Government imposed constraints on the export to the PRC of certain items on the CCL. Section 902(a)(4) of the Foreign Relations Authorization Act for Fiscal Year 1990-1991, Public Law 101-246, suspends the issuance of licenses under Section 6(n) of the EAA for the export of any crime control or detection instruments or equipment to the PRC."

[41] *Crime Control and Detection*. EAR §742.7. http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=45e6c763621277af6b2e198439bf50fe&r=PART&n=15y2.1.3.4.26#15:2.1.3.4.26.0.1.7..

[42] Bureau of Indusrty and Security, US Department of Commerce. 2014. *2014 Report on Foreign Policy-Based Export* Controls. 16. Bureau of Industry and Security. http://www.bis.doc.gov/index.php/forms-documents/doc_download/870-bis-foreign-policy-report-2014.

[43] Open Society Policy Center. 2013. *Export Control Reform: US Weapons at Greater Risk of Being Used in Human Rights Violations Congress's Carefully Legislated Web of Statutes Being Dismantled by Regulatory Fiat.* Washington, DC: Open Society Policy Center. http://opensocietypolicycenter.org/wp-content/uploads/Arms-Export-Reforms-Undermine-Congress-Human-Rights-Protections.pdf.

Limitation on assistance to security forces. 22 USC § 2378d. http://law.justia.com/codes/us/2010/title22/chap32/subchapiii/parti/sec2378d.

[44] Bureau of Indusrty and Security, US Department of Commerce. 2014. *2014 Report on Foreign Policy-Based Export* Controls. Bureau of Industry and Security. http://www.bis.doc.gov/index.php/forms-documents/doc_download/870-bis-foreign-policy-report-2014.

[45] Bureau of Democracy, Human Rights and Labor, US Department of State. 2013. "Country Reports on Human Rights Practices for 2013 Secretary's Preface." Accessed March 18, 2014. http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper.

[46] Bureau of Democracy, Human Rights and Labor, US Department of State. 2013. "Country Reports on Human Rights Practices for 2013 Secretary's Preface." Accessed March 18, 2014. http://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper.

[47] Silver, Vernon. 2012. "Cyber Attacks on Activists Traced FinFisher Spyware of Gamma. *Bloomberg,* July 25. http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html.

[48] Based on information provided by the US Department of Commerce

[49] Bureau of Industry and Security, US Department of Commerce. 2014. *2014 Report on Foreign Policy-Based Export* Controls. 90. Bureau of Industry and Security. http://www.bis.doc.gov/index.php/forms-documents/doc_download/870-bis-foreign-policy-report-2014.

[50] See Comments to the U.S. Department of State submitted in response to Public Notice 8086 by Access Now, the Center for Democracy and Technology, Collin Anderson, the Committee to Protect Journalists, and the New America Foundation's Open Technology Institute on January 12, 2013, with regard to the guidance on "sensitive technology" available at http://oti.newamerica.net/publications/resources/2

013/comments_regarding_sensitive_technologies_guidance.

[51] Bureau of Economic and Business Affairs, US Department of State. 2012. "Iran Sanctions Contained in the Iran Threat Reduction and Syria Human Rights Act (ITRSHRA)." Last modified September 28. http://www.state.gov/e/eb/rls/fs/2012/198393.htm.

[52] Executive Order 13606 of April 22, 2012, Blocking the Property and Suspending Entry into the United States of Certain Persons with Respect to Grave Human Rights Abuses by the Governments of Iran and Syria Via Information Technology. *Compilation of Presidential Documents.* http://www.gpo.gov/fdsys/pkg/DCPD-201200294/pdf/DCPD-201200294.pdf.

[53] Bureau of Industry and Security, US Department of Commerce. 2014. *2014 Report on Foreign Policy-Based Export* Controls. Bureau of Industry and Security. http://www.bis.doc.gov/index.php/forms-documents/doc_download/870-bis-foreign-policy-report-2014.

[54] World Trade Organisation, 2013, Rank in World Trade, 2012. See: The World Trade Organization. "Trade Profiles: Germany, United Kingdom, United States." Last modified September. http://stat.wto.org/CountryProfile/WSDBCountryPFView.aspx?Language=E&Country=US,GB,DE.

[55] The main importers and exporters of major arms, 2008–2012. Retrieved from: Stockholm International Peace Research Institute. 2013. *SIPRI Yearbook 2013: Armaments, Disarmament and International Security.* Oxford: Oxford University Press. http://www.sipri.org/yearbook/2013/05.

[56] UK Ministry of Defence. 2012. *National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security.* 7. Surrey: Crown Copyright. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27390/cm8278.pdf.

[57] Jackson, Susan T. 2011. *SIPRI assessment of UK arms export subsidies – For CATT.* http://www.caat.org.uk/resources/publications/economics/subsidies-sipri-2011.pdf.

[58] Privacy International. "Surveillance Industry Index." Accessed March 18, 2014. https://www.privacyinternational.org/sii/.

[60] UK Trade and Investment. 2013. "Case Study Technology company helped to secure millions of pounds of business." Last modified April 25. https://www.gov.uk/government/case-studies/technology-company-helped-to-secure-millions-of-pounds-of-export-business.

[61] UK Department for Business, Innovation & Skills. 2012. "Consolidated EU and national arms export licensing criteria." Last modified November 21. https://www.gov.uk/government/publications/consolidated-eu-and-national-arms-export-licensing-criteria.

[62] UK Department for Business, Innovation & Skills. 2012. "Consolidated EU and national arms export licensing criteria." Last modified November 21. https://www.gov.uk/government/publications/consolidated-eu-and-national-arms-export-licensing-criteria.

[63] UK Department for Business, Innovation & Skills. 2013. "Notice to Exporters 2013/10: Export Control (Amendment) Order 2013." Last modified March 19. http://blogs.bis.gov.uk/exportcontrol/general-awareness/notice-to-exporters-201310-export-control-amendment-order-2013/.

[64] United Kingdom. 2008. "Customs : The Export Control Order 2008, Statutory Instrument, 2008 No. 2231." http://www.legislation.gov.uk/uksi/2008/3231/pdfs/uksi_20083231_en.pdf.

[65] European Union. 2012. "Notices From Member States." *Official Journal of the European Union* C67/1. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:067:0001:0063:EN:PDF

[66] European Union. 2005. "Council Regulation (EC) No 1236/2005 of 27 June 2005. Concerning trade in certain goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment." *Official Journal of the European Union* L200/1. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:200:0001:0019:EN:PDF

[67] United Kingdom, 2006. "Explanatory Memorandum to the Export of Radioactive Sources (Control) Order 2006 No.1846." http://www.legislation.gov.uk/uksi/2006/1846/pdfs/uksiem_20061846_en.pdf.

[68] United Kingdom. 2002. Export Control Act 2002, Schedule 1. http://www.legislation.gov.uk/ukpga/2002/28/schedule

[69] United Kingdom. 2006. "Explanatory Memorandum to the Export of Radioactive Sources (Control) Order 2006 No.1846." http://www.legislation.gov.uk/uksi/2006/1846/pdfs/uksiem_20061846_en.pdf.

[70] UK House of Lords, December 2011, WA, Col. WA134 http://www.publications.parliament.uk/pa/ld201011/ldhansrd/text/111205w0001.htm.

[71] Cable, Vince. 2013. "Letter to the Chair of the Committees from the Rt Hon Vince Cable MP, Secretary of State for Business, Innovation and Skills." Last modified April 16. http://www.publications.parliament.uk/pa/cm201314/cmselect/cmquad/205/205we50.htm.

[72] UK Export Control Organisation, email message to the author. November 15, 2013.

[73] Hague, William. 2012. "Letter to the Chair of the Committees from the Rt Hon William Hague MP, First Secretary of State and Secretary of State for Foreign & Commonwealth Affair." http://www.publications.parliament.uk/pa/cm201314/cmselect/cmquad/205/205ii11.htm.

[74] Export Control Act 2002 (UK) http://www.legislation.gov.uk/ukpga/2002/28/pdfs/ukpga_20020028_en.pdf

[75] United Kingdom. 2010. *Customs : The Export Control (Amendment) (No. 3) Order, Statutory Instrument*. http://www.legislation.gov.uk/uksi/2010/2843/pdfs/uksi_20102843_en.pdf.

[76] Reprieve. 2010. "High Court hears arguments on UK government decision not to ban further exports to the United States of execution drug sodium thiopental." Last modified November 17. http://www.reprieve.org.uk/press/2010_11_17_High_Court/.

Department for Business Innovation & Skills. 2011. "Government bans export of lethal injection drugs to US." Last modified April 14. http://news.bis.gov.uk/content/Detail.aspx?ReleaseID=419199&NewsAreaID=2.

[77] Committees on Arms Export Controls, UK Parliament. 2013. *Scrutiny of Arms Exports and Arms Control (2013).* Annex 3. http://www.publications.parliament.uk/pa/cm201314/cmselect/cmquad/205/205ii_04.htm.

[78] See Baker, R, and R Bohlig. "Control of Exports-A Comparison of the Laws of the United States, Canada, Japan, and the Federal Republic of Germany, The." *Int'l L.* (1966) and Burkemper, JI. "Export Verboten: Export Controls in the United States and Germany." *S. Cal. L. Rev.* (1993).

[79] See Burkemper, JI. "Export Verboten: Export Controls in the United States and Germany." *S. Cal. L. Rev.* (1993).

[80] See Corcoran, DD. "Practical Failure of German Export Control Law: A Lesson in Modern Trade, The." *Fordham Int'l LJ* (1992), Jones, JP, and EN Wagner. "Poision Gas Proliferation: Paradox, Politics, and Law." *Loy. LA Int'l & Comp. LJ* (1992), Kellman, B. "Bridling the International Trade of Catastrophic Weaponry." *Am. UL Rev.* (1993) and Lundin, SJ, and T Stock. "Chemical and Biological Warfare: Developments in 1990." *SIPRI, SIPRI Yearbook* (1991).

[81] See Nassauer, Otfried, and Christopher Steinmetz. *„Made in Germany" inside Komponenten – Die Vergessenen Rüstungsexporte*. Berlin: BITS, Oxfam Deutschland, 2005.

[82] Melchior, OJ. "Compliance in Der Außenwirtschaft: Exportkontrolle." *Compliance in Der Unternehmerpraxis* (2013).

[83] See for example Erste Verordnung zur Änderung der Außenwirtschaftsverordnung (1. AWVÄndV k.a.Abk.) V. v. 13.12.2013 BAnz AT 20.12.2013 V1 which can be accessed at http://www.buzer.de/gesetz/11051/index.htm .

[84] For further details, see: Silver, Vernon and Ben Elgin. 2011. "Area SpA May Exit Syrian Monitoring Project." *Bloomberg,* November 8. http://www.bloomberg.com/news/2011-11-09/syrian-monitoring-project-may-end-as-italy-firm-weighs-options.html.

[85] See Lischka, Konrad. "Überwachungssoftware: Deutschland Kontrolliert Trojaner-Exporte Nicht - SPIEGEL ONLINE." *DER SPIEGEL*, 2012. http://www.spiegel.de/netzwelt/netzpolitik/ueberwachungssoftware-deutschland-kontrolliert-trojaner-exporte-nicht-a-850357.html.

[86] See Meister, Andre. "Internes Dokument Belegt: Innenministerium Gibt Fast 150.000 Euro Für Staatstrojaner FinFisher/FinSpy Aus." *Netzpolitik*, 2013. https://netzpolitik.org/2013/internes-dokument-belegt-innenministerium-gibt-fast-150-000-euro-fur-staatstrojaner-finfisherfinspy-aus/ and Nassauer, Otfried, and Christopher Steinmetz. *„Made in Germany" inside Komponenten – Die Vergessenen Rüstungsexporte*. Berlin: BITS, Oxfam Deutschland, 2005.

[87] See Lustermann, Henning, and Markus Witte. "Compliance in Der Außenwirtschaft: Exportkontrolle." *Compliance in Der Unternehmerpraxis* (2008): 85–98.

[88] See Melchior, OJ. "Compliance in Der Außenwirtschaft: Exportkontrolle." *Compliance in Der Unternehmerpraxis* (2013).

[89] See Melchior, OJ. "Compliance in Der Außenwirtschaft: Exportkontrolle." *Compliance in Der Unternehmerpraxis* (2013).

[90] Bromley, Mark. 2012. "The Review of the EU Common Position on Arms Exports: Prospects For Strengthened Controls." *EU Non-Proliferation Consortium*. Accessed March 18, 2014. http://www.sipri.org/research/disarmament/eu-consortium/publications/publications/non-proliferation-paper-7.

[91] ibid

[92] Council of the EU. 2009. *User's Guide to Council Common Position 2008/944/CFSP Defining Common Rules Governing the Control of Exports of Military Technology and Equipment*. http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%209241%202009%20INIT&r=http%3A%2F%2Fregister.consilium.europa.eu%2Fpd%2Fen%2F09%2Fst09%2Fst09241.en09.pdf.

[93] European Union. 2012. "Notices from European Union Institutions, Bodies, Offices and Agencies." *Official Journal of the European Union*. C386/1. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:386:0001:0431:EN:PDF.

[94] European Union. 2012. "Regulation (EU) No 388/2012 of the European Parliament and the Council of 19 April 2012 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 of the European* Union. L129/12. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:129:0012:0280:EN:PDF.

[95] Bauer, Sibylle and Mark Bromley. 2013. "Dual-Use and Arms Trade Controls." *SIPRI Yearbook 2013: Armaments, Disarmament and International Security*, 421-468 Oxford: Oxford University Press.

[96] European Parliament, European Union. 2012. *Position adopted at first reading on 23 October 2012 view to the adoption of Regulation (EU) No .../2012 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 (EP-PE_TC1-COD(2011)0310)*. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2012-383.

[97] European Commission, European Union. 2012. *Commission Communication on the action taken on opinions and resolutions adopted by Parliament at the October 2012 I and II part-sessions*. http://www.europarl.europa.eu/oeil/spdoc.do?i=21891&j=0&l=en.

[98] British export authorities, correspondence with the author. January 14, 2014.

[99] European Parliament. 2011. "Controlling dual-use exports." Last modified September 27.

http://www.europarl.europa.eu/news/en/newsroom/content/20110927IPR27586/html/Controlling-dual-use-exports.

[100] ibid

[101] European Commission. 2008. "Sanctions or Restrictive Measures." Last modified spring 2008. http://eeas.europa.eu/cfsp/sanctions/docs/index_en.pdf#6.

[102] [102] UK Department for Business, Innovation and Skills. 2013. "Explanatory Memorandum to the Export Control (Syria Sanctions) Order 2013." Accessed March 18, 2014. http://www.legislation.gov.uk/uksi/2013/2012/pdfs/uksiem_20132012_en.pdf.

[103] European Union. 2012. "Notices From Member States." *Official Journal of the European Unio*n, C67/1. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:067:0001:0063:EN:PDF.

[104] Council Regulation (EU) No 264/2012 of 23 March 2012 amending Regulation (EU) No 359/2011 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Iran, March 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:087:0026:0036:EN:PDF

[105] European Union. 2012. "Notices From Member States." *Official Journal of the European Union,* C283/4. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:283:0004:0004:EN:PDF

[106] European Union. 2005. "Council Regulation (EC) No 1236/2005 of 27 June 2005.

Concerning trade in certain goods which could be used for capital punishment, torture or other cruel, inhuman or degrading treatment or punishment." *Official Journal of the European Union* L200/1. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:200:0001:0019:EN:PDF

[107] Wassenaar Arrangement. 2003. "Statement of Understanding on Control of Non-Listed Dual-Use Items (1) (Agreed at the 2003 Plenary)."

http://www.wassenaar.org/guidelines/docs/Non-listed_Dual_Use_Items.pdf.

[108] European Union. 2009. "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*. L134/1. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF.

[109] UK Department for Business, Innovation & Skills. 2012. *Response from Her Majesty's Government to the European Commission Green Paper on the dual-use export control system of the European Union*. Surrey: Crown Copyright. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/32007/12-509-eco-response-eu-green-paper-dual-use.pdf.

[110] Committees on Arms Export Controls. 2012.

"Scrutiny of Arms Exports (2012): UK Strategic Export Controls Annual Report 2010, Quarterly Reports for July to December 2010 and January to September 2011, the Government's Review of arms exports to the Middle East and North Africa, and wider arms control issues." Accessed March 18, 2014. http://www.publications.parliament.uk/pa/cm201213/cmselect/cmbis/419/41910.htm.

[111] European Union. 2009. "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,* L134/1. http://trade.ec.europa.eu/doclib/docs/2009/june/tradoc_143390.pdf.

[112] European Union, Notices From Member States, Official Journal of the European Union, C67/1, March 2012. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:067:0001:0063:EN:PDF

[113] European Union. 2012. "Notices From Member States." *Official Journal of the European Unio*n, C67/1. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:067:0001:0063:EN:PDF.

[114] Elgin, Brad and Vernon Silver. 2011. "Syria Crackdown Gets Italy Firm's Aid With US-Europe Spy Gear", *Bloomberg*, November 3. http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html.

[115] Based on SIPRI data, available at: Stockholm International Peace Research Institute. 2013. *SIPRI Yearbook 2013: Armaments, Disarmament and International Security.* Oxford: Oxford University Press. http://www.sipri.org/yearbook/2013/05 http://www.sipri.org/yearbook/2013/05.

[116] Wassenaar Arrangement. 2005. "Criteria for the Selection of Dual-Use Items (as updated at the December 2005 Plenary)." http://www.wassenaar.org/controllists/2005/Criteria_as_updated_at_the_December_2005_PLM.pdf.

[117] Reports from the Business, Innovation and Skills, Defence, Foreign Affairs and International Development Committees Session 2013-14 Strategic Export Controls: Her Majesty's Government's Annual Report for 2011, Quarterly Reports for 2011 and 2012, and the Government's policies on arms exports and international arms control issues

Response of the Secretaries of State for Defence, Foreign and Commonwealth Affairs, International Development and Business, Innovation and Skills, para. 88, October 2013. http://www.official-documents.gov.uk/document/cm87/8707/8707.pdf (p. 37)

[118] Privacy International. 2014. "Gamma Group." Surveillance Industry Index. https://www.privacyinternational.org/sii/gamma_group/.

[119] Retrieved from: https://www.documentcloud.org/documents/409278-147-hackingteam-rcs.html#document/p2/a68009

[120] Retrieved from: https://www.documentcloud.org/documents/810501-769-gamma-group-product-list-finfisher.html#document/p1/a132141

[121] Wikipedia. 2013. "E-carrier." Last modified December 5. http://en.wikipedia.org/wiki/E-carrier.

Wikipedia. 2014. "T-carrier." Last modified February 26. http://en.wikipedia.org/wiki/T-carrier.

[122] Wassenaar Arrangement. 2006. "Best Practices for Implementing Intangible Transfer of Technology Controls (Agreed at the 2006 Plenary)." http://www.wassenaar.org/guidelines/docs/ITT_Best_Practices_for_public_statement.pdf.

[123] Wassenaar Arrangement. 2013. "Dual-Use List." Last modified April 12. http://www.wassenaar.org/controllists/2013/WA-LIST%20%2813%29%201/02%20-%20WA-LIST%20%2813%29%201%20-%20GTN%20and%20GSN.doc.

[124] Copyright restrictions do not remove "technology" or "software" from being "in the public domain".

[125] Wassenaar Arrangement. 2013. "Definitions." Last Modified April 12. http://www.wassenaar.org/controllists/2013/WA-LIST%20%2813%29%201/16%20-%20WA-LIST%20%2813%29%201%20-%20DEF.doc.

[126] Technology is defined as: Specific information necessary for the "development", "production" or "use" of a product. The information takes the form of technical data or technical assistance.

[127] Here, "in the public domain" is defined as: "technology" or "software" which has been made available without restrictions upon its further dissemination.

[128] Basic scientific research is defined as: Experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.

DIGITALE GESELLSCHAFT

Office
Sophienstraße 5
10178 Berlin
Germany
Phone +49 (0) 30 6891 6575

PRIVACY INTERNATIONAL

Office
62 Britton Street
London, EC1M 5UY
United Kingdom
Phone +44 (0) 20 3422 4321

Main Office
1899 L Street, NW
Suite 400
Washington, DC 20036
United States of America
Phone +1 202 986 2700
Fax +1 202 986 3696

New York Office
199 Lafayette Street
Suite 3B
New York, NY 10012
United States of America

NEW AMERICA FOUNDATION

WWW.NEWAMERICA.NET