PRIVACY INTERNATIONAL

The Global Surveillance Industry

A report by Privacy International
July 2016

PRIVACY INTERNATIONAL

REMOTE CONTROL
Examining changes in military engagement

The production of this report was supported by a grant from Remote Control, a project of the Network for Social Change hosted by Oxford Research Group (registered charity number: 299436)

Table of Contents

Executive Summary

This report is about electronic surveillance technologies used to identify, track, and monitor individuals and their communications for intelligence gathering and law enforcement purposes.

Technological developments since the Cold War, during which espionage and the monitoring of civilians was widespread, has increased the intrusiveness and power of surveillance. The ability to monitor the communications of entire groups and nations on a mass scale is now a technical reality, posing new and substantially more grave human rights issues. Recent reforms of surveillance laws undertaken across political systems with significant checks and balances show how easily surveillance capabilities can outstrip the ability of laws to effectively regulate them. In non-democratic and authoritarian systems, the power gained from the use of surveillance technologies can undermine democratic development and lead to serious human rights abuses. Opposition activists, human rights defenders, and journalists have been placed under intrusive government surveillance[1][2][3] and individuals have had their communications read to them during torture.[4] State agencies are also utilizing technologies used for surveillance for offensive and military purposes as well as espionage.

This report aims to map modern electronic surveillance technologies, their trade, the companies which manufacture and export them, and the regulation governing their trade. By doing so, it aims to increase understanding about the surveillance industry in order to foster accountability as well as the development of comprehensive safeguards and effective policy.

While a number of studies and media reports since the 1970s have highlighted the role of the private sector in developing and selling surveillance technologies and the use of specific types, there is limited data about the surveillance industry, and obtaining reliable data is challenging. The information that is currently available comes from largely from investigative reporting, whistleblowers, and government transparency reports.

Privacy International has compiled the information that is available within the Surveillance Industry Index (SII), a database consisting of data and documentation about surveillance technologies and companies, as well as reports about the use and sale of specific technologies.

1 https://www.privacyinternational.org/node/816

2 https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/

3 http://apnews.excite.com/article/20150807/lt--ecuador-hacking_the_opposition-18a465a3dd.html

4 http://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking

This report begins by presenting a historical overview of the surveillance industry since the 1970s, including significant policy developments and disclosures of information.

After outlining the sources and methods used for the report, it then presents a typology for different corporate actors involved in surveillance, and data relating to the geographic distribution of the 528 surveillance companies in the SII. These companies are overwhelmingly based in economically advanced, large arms exporting states, with the United States of America (USA), United Kingdom (UK), France, Germany, and Israel comprising the top five countries in which the companies are headquartered. An overview of the specific types of surveillance technologies included in the SII is then introduced, while a more detailed explanation of the specific types is provided in the annex.

The report then presents an analysis of the surveillance industry in Israel, the US, UK, Germany, and Italy, including an analysis of known exports as well as industry characteristics. An analysis of 152 reported imports of surveillance technologies into the Middle East and North Africa region follows.

The next section provides an overview of how some of these technologies can be used for espionage and in military applications, either being directly used in warfare, for military intelligence, or by intelligence agencies for military end-users. It also describes how advanced intelligence agencies are developing and utilizing the surveillance capabilities of foreign states.

A discussion on policy developments aimed at regulating the trade in some of the technologies, including through industry self-regulation, sanctions, and export controls, is followed by the conclusion.

Introduction

In 1979, New Scientist reported on the role of the State Research Centre, the "most feared and hated building" in Uganda, in mass killings during the eight year rule of dictator Idi Amin.[5] Established in 1973, the centre was reportedly used by some 1500 agents to spy on and identify individuals, and subsequently to torture, terrorise, and kill "virtually anyone who fell foul of them or Amin". At the time, a police mortician who had kept records of the subversives that had been killed by the agents, said that he had seen over 5000 corpses in the past two years, a number that he said was only the "tip of the iceberg". In total, Amnesty International charged the State Research Centre together with other agencies with responsibility for the killing of between 100,000 and 500,000 people during Amin's time.[6]

The operational capacity of the Centre and its agents and their ability to assert political and social control was directly enabled by various electronic technologies originating in the United Kingdom. A British company, Security Systems International Ltd, sold the unit telephone tapping devices, radio telecommunications and radio detection devices. Despite the subsequent criticism and risk of facilitating human rights abuses and killings by the provision of such surveillance equipment, the provider at the time contested that there was nothing that his company had done that was legally wrong, and that their operations had been vetted "16 different ways backwards and forwards" by the government.[7]

Over 30 years later, Privacy International again reported on the role that a different British company had played in providing Ugandan agencies with surveillance equipment.[8] The report found that the Ugandan military had in 2012 used technology sold by a British company as the 'backbone' of a secret operation to spy on leading opposition members, activists, elected officials, intelligence insiders and journalists. According to a classified memo, the police and military deployed the technology specifically to "crush...civil disobedience" and "cra[ck] down [on] the rising influence of the opposition" by "blackmailing them". In 2015, further media reports claimed that the Ugandan government had also procured a monitoring centre from an Israeli company designed to monitor the entirety of the nation's internet traffic.[9]

5 Harriman, E, "The British Connection", New Scientist, 10 May 1979.

6 Amnesty International, "The Repression Trade", Revised Briefing Paper, January 1981, available at <https://www.amnesty.org/download/Documents/200000/pol340051981en.pdf>

7 Harriman, E, "The British Connection", New Scientist, 10 May 1979.

8 https://www.privacyinternational.org/node/656

9 Africa Intelligence,"Museveni commits $85.5 million to monitor the Web", N°1414 - 06/11/2015 <http://www.africaintelligence.com/ION/politics-power/2015/11/06/museveni-commits-dollars85.5%C2%A0million-to-monitor-the-web,108110202-ART>

Little was known about the trade in such surveillance technologies at the time of the State Research Centre scandal. In 1979, Michael T Klare, then fellow of the Institute for Policy Studies in Washington DC, dubbed the trade in technologies used for social-control the "International Repression Trade", an industry on which there was little reliable data, but which appeared to be growing.[10] Spurred by the belief of Western powers that any erosion of government authority in the Third World nations would undermine the process of modernisation, the Western powers responded by strengthening the social-control capabilities of the prevailing regime. "Faced with a choice between the continuation of the status quo and a major social upheaval culminating in the rise of unknown leaders, who may or may not respect the trade and investment policies of their predecessors, most Western powers will opt for the status quo despite the risks involved."[11]

The industrialising nations themselves, experiencing traumas related to economic factors and ethnic and religious strife, were responding by expanding their military-police sector, and clamping down on popular movements using more aggressive and systematic methods:

"As the opposition expands and becomes more experienced in clandestine operations, traditional police methods prove increasingly ineffective and the security forces are obliged to use more and more sophisticated equipment to gain information on dissident groups. New eavesdropping and surveillance technologies must be introduced to locate opposition cells, and computers are needed to process all the data provided by spies and informers."[12]

Klare noted at the time that this trade was not just confined to the Western powers and their allies, but also being conducted between NATO countries, and between the Socialist powers and their allied countries. Further, the trade was not just conducted by private companies selling to international customers, but further enabled through the establishment by Western governments of special programs to facilitate the procurement of such equipment to security forces of allied countries, either directly or through financial assistance. These programs came under the rubric of military and security assistance, counter narcotics cooperation, and training and technical assistance delivered to security forces.

Echoing Klare's bleak assessment that without companies' exports being restrained the "balance of power will continue to favour the forces of oppression", Amnesty International in 1980 recognised this demand by "militarised regimes in the Third World" for "surveillance technologies that are developed and manufactured in the arms exporting countries".[13]

10 Klare, M, "The International Repression Trade", Bulletin of Atomic Scientists, November 1979.

11 Ibid p23

12 ibid p23

13 Amnesty International, "The Repression Trade", Revised Briefing Paper, January 1981, available at https://www.amnesty.org/download/Documents/200000/pol340051981en.pdf

Amnesty International argued that regimes were seeking "technological solutions" to situations that they could not resolve by more normal political means. By 1981, electronic systems developed in Britain were being used for surveillance and social control not just in Uganda, but also by the secret police in Saudi Arabia, in Iran during the rule of the Shah, apartheid South Africa, and even in the Soviet Union.[14] Amnesty International charged at the time that far from only having a responsibility where a direct connection can be made between the product and serious human rights abuses, the UK was directly implicating itself in human rights abuses in the recipient country by authorising and in some instances promoting exports. As well as encouraging what it called "the militarisation of the political system" in recipient countries, Amnesty argued that:

"The supply of military and security equipment to a government that is using or that is preparing to use repression against some part of its own population represents a deliberate intervention in the internal politics of that country, on the side of the repressive government against those that it conceives to be its enemies."[15]

Amnesty had called out a "grey area" consisting of products not specially designed for military use but nonetheless used for repression to become subject to export licensing restrictions, meaning that exporters who were selling tools of repression to security forces abroad would require a government license to do so.

The export of surveillance capabilities across the world, and particularly by large arms-exporting States, has been subject to various analyses since then.

In 1995, Privacy International published Big Brother Incorporated[16], a study of the international trade in surveillance technologies and what appeared to be the increasing role of companies in the arms industry in facilitating surveillance capabilities across the world.

In 1998, Steve Wright conducted a review of technologies for political control for the European Parliament, including technologies allowing bugging, telephone monitoring, and the emergence of new forms of local, national and international communications interceptions networks and the creation of human recognition and tracking devices.[17] Warning of an "arsenal of new weapons and technologies of political control [that] has already been developed or lies waiting on the horizon for a suitable opportunity to find useful work", Wright called for "urgent action...to ensure European technology of political control does not get into the hands of tyrannical and repressive regimes".[18]

14 Ibid p17

15 ibid p16

16 http://cd.textfiles.com/group42/CRYPTO/MISC/COMPANIE.HTM

17 Wright, S, "An Appraisal of Technologies of Political ControL", 6 January 1998"ht available at <http://cryptome.org/stoa-atpc.htm#4>

18 Ibid p59

In 2004, Amnesty International released an analysis of European export licensing restrictions that applied to surveillance and interception technologies, prompted by evidence that European companies and States had provided such technologies to a range of repressive regimes, including Turkmenistan and Saudi Arabia.[19] Amnesty recommended that "All EU governments and the European Commission should review their export control policies with regard to the export of 'dual-use' goods... to ensure that that the transfer of sophisticated communication and surveillance systems is not permitted to countries where such systems are likely to be used to facilitate human rights violations."[20]

Despite these calls however, efforts to comprehensively stop the transfer of such surveillance capabilities to authoritarian regimes are difficult to quantify. When the various government agencies fell during the Arab Awakening, journalists and activists for the first time got an insight into the apparatus that underpinned their surveillance and control mechanisms, finding it to be in large part enabled by European and US and technologies.[21] These companies had provided the various government agencies across the Middle East and North Africa with sweeping surveillance capabilities, including internet and phone monitoring technologies that can be used to monitor entire populations, undermining the human right to privacy and facilitating a range of other abuses.[22]

This report focuses on the provision by companies of electronic surveillance products to security forces end-users for the purpose of law enforcement and intelligence gathering. Unless otherwise stated, "surveillance technology" will refer to these purposes in this report.

The use of these techniques has become central to law enforcement and intelligence agencies. Partly driven by the rise of non-state threats as a key policy driver since the Cold War, it is also spurred by technological developments, weak regulatory mechanisms, the relatively low expense of such techniques, and their preference for policy makers to human intelligence gathering techniques.

19 Amnesty International, "Undermining Global Security: The European Union's Global Arms Exports", 2004, Available at <http://www.amnesty.eu/static/documents/Text_ACT300032004.pdf>

20 Ibid p64

21 Wagner, B, "Exporting Surveillance & Censorship Technologies", Hivos, January 2012, available at <https://www.hivos.org/sites/default/files/exporting_censorship_and_surveillance_technology_by_ben_wagner.pdf>

22 ibid

Although the focus of this report is on civilian surveillance technologies, they also have military applications, either being directly used in warfare, for military intelligence, or by intelligence agencies for military end-users. As described below, many of these technologies are also used for espionage by nation state authorities or associated groups. Equipment used to monitor demonstrations is being used to facilitate drone strikes, the data gained from nationwide internet monitoring tools is being used identify military targets and their relationships, technology similar to that used by police to hack into a mobile phone to gather evidence is being used for espionage and sabotage.

This report aims to map these modern surveillance technologies, their trade, the companies which manufacture and export them, and their regulation. By doing so, it aims to not only provide much-needed exposure and accountability onto an industry which strives to operate in secrecy, but to also facilitate a better understanding of modern State law enforcement, intelligence, and military practices. It also aims to provide a foundation for further research for interpreting the modern defence and security industry, international security, and modern warfare.

Sources and Methods

Analyses into the arms trade, the arms production industry, and military expenditure are based on a range of open sources and official publications, including national and international arms trade registers, national export licensing data, annual company reports, and publications of contract awards. These are generally cross referenced with media reporting and trade journals.

Reliable data related to intelligence capabilities is extremely difficult to access as it is regarded as a matter of national security to keep information secret. It is therefore largely classified and exempt from public reporting obligations and freedom of information rules.

Public access to knowledge about contemporary North American and European intelligence agencies has largely relied on investigative research from among others Campbell (1988),[23] Hager (1996),[24] Bamford (1983, 2008),[25] individuals submitting material to platforms such as Cryptome and Wikileaks, whistleblowers such as William Binney, Thomas Drake, Thomas Tamm, and most recently Edward Snowden, as well as accounts by former government officials and declassified materials.

Access to reliable data about the surveillance industry suffers from these same difficulties, and is made even more difficult by trade secrecy rules. Information about company data, surveillance technology, and transfers have been compiled using the sources and methods described below. However, there are significant difficulties and limitations on carrying out a reliable industry analysis using the limited data currently available. This report nonetheless aims to analyse the information predominantly in the English language that is publicly available. It is hoped that researchers, journalists, academics, and government officials will build on this analysis.

In addition to the sources and methods described below, Privacy International carries out extensive primary investigative research, including regular field work in high risk environments, to gather information about the surveillance industry. It also consults regularly with journalists, researchers, and activists, as well as individuals within industry and government officials.

23 http://cryptome.org/jya/echelon-dc.htm

24 http://www.nickyhager.info/category/books/

25 http://www.amazon.com/The-Puzzle-Palace-Intelligence-Organization/dp/0140067485

Company Data

The purpose of this report is not to analyse the entirety of the private sector's role in the intelligence and law enforcement sector. It focuses only on companies which produce or market a specific surveillance technology, described in the Surveillance Technologies section. It does include Original Equipment Manufacturers (OEMs) which specially design or market their products for surveillance purposes, but not companies whose products have wider applications, for example in internet network monitoring for performance purposes. Although prime contractors and private military and security companies (PMSCs) play a pivotal and under-explored role in the facilitation and promotion of surveillance capabilities, companies which only supply staff or consultancy services are not included in this analysis.

Only companies which sell to government agencies or telecommunications companies for government purposes are included. Companies which sell relatively unsophisticated surveillance technologies on the internet are not included. As a result, the companies which are included either do not widely market their technologies publicly or purposefully conceal any details about their products. Many have a minimal online presence or are allusive as to the exact capabilities and purpose of their products.

Privacy International has for several years been collecting information on surveillance companies and technologies within the Surveillance Industry Index (SII). The SII is the world's largest publicly accessible database on the commercial surveillance sector, featuring 528 companies as of May 2016. The majority of the companies have been initially identified because they have attended a military, security, or surveillance trade fair that has also been attended by Privacy International. The remainder of the companies were identified through online searches and references in open sources, including media and company registration data.

Because the trade fairs have focused on intelligence and communications surveillance, the companies featuring in SII are predominantly involved in communications surveillance, meaning that companies which produce audio and video surveillance, forensics, and biometrics are under-represented.

Investigative reporting and open source analyses are also used, for example Wright (1998, 2005, 2006)[26] and Privacy International (1995).[27]

Other sources include online databases, such as BuggedPlanet[28] which keep records on publicly available information on a large amount of surveillance companies. In 2015, the European Commission commissioned the Stockholm International Peace Research Institute (SIPRI) to conduct a data collection project specifically on surveillance technologies as part of a review of the EU Dual Use regulation, which governs the export of some surveillance technologies.[29] In 2014, an apparently vetted member-only online trade magazine was launched purporting to review and analyse surveillance technologies and companies worldwide, although its sources, methods, contributors, and revenue structure are undisclosed.[30]

26 http://www.leedsbeckett.ac.uk/staff/dr-steve-wright/

27 Privacy International (Ed.) (1995) Big Brother Incorporated - A report On the International Trade in Surveillance Technology and Its Links To The Arms Industry. 1st ed. Vol. 1, November. Privacy International, London.

28 www.buggedplanet.info

29 http://www.europarl.europa.eu/RegData/etudes/STUD/2015/535000/EXPO_STU(2015)535000_EN.pdf

30 www.insidersurveillance.com

Surveillance Technologies

Privacy International has collected thousands of individual security equipment brochures and other material across various trade shows, and has as of April 2016 made 1534 of the most relevant brochures publicly available. The trade shows attended have taken place worldwide, including Western Europe, South Africa, the Middle East, and South East Asia. Outside of South Africa however, the trade shows have all been located within one of the 37 countries with whose intelligence agencies the US National Security Agency has an approved relationship on the collection of signals intelligence.[31] This means that technologies developed in China and Russia are likely underrepresented, although companies from these countries do exhibit at the majority of international trade shows. WikiLeaks' has also published a significant amount of company promotional documents and internal material as part of its Spy Files releases.[32]

The disclosures related to the NSA and its intelligence partners beginning in 2013 made possible by Edward Snowden, a contractor with Booz Allen Hamilton, are available widely online and used throughout to inform analysis.

31 http://www.duncancampbell.org/content/nsa-inside-five-eyed-vampire-squid-internet

32 https://wikileaks.org/spyfiles/

Transfer Data

Reliable data about sales and exports of surveillance technology is extremely limited. Privacy International has developed a database of all transfers of communications surveillance technology that it has identified in the public domain, largely in the English language. This does not include transfers of non-communications surveillance technology such as biometrics and video/audio surveillance. As of April 2016, there are 607 such transfers. The database contains data from open sources and government data.

Open sources include reporting by media, NGOs, and research institutes, which to the best of Privacy International's knowledge are accurate. Some data has been made available through technical research, for example that conducted within the Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto, Canada.

Government data is almost exclusively made up of national export licensing data, one of the best sources for government data, although only Finland, the United Kingdom, and Switzerland currently release useful statistics and only since relatively recently. Further, export licensing data means that permission has been provided to an exporter to export technology which falls within the control language parameters outlined within the specific export control category. It is not a definitive indication that a transfer has taken or will take place. An extremely limited amount of government data has been released through freedom of information requests and public procurement records.

Surveillance Companies

The modern electronic communications surveillance industry evolved from the commercialisation of the internet and digital telecommunications networks during the nineties, before which the level and sophistication of electronic surveillance in the civilian realm was necessarily limited by levels of access to sophisticated networks and devices. Nonetheless, there is a well documented history of electronic surveillance during the Cold War, including the collection of Signals Intelligence (SIGINT) and Communications Intelligence (COMINT) by satellites,[33] aircraft, and submarine cable taps[34] and the wiretapping of civilian telephones by intelligence agencies across the Warsaw Pact and NATO countries.[35]

As networks expanded and modernised during the nineties, legislation and technical protocols were enacted in Europe and the US to guarantee government access. The 1994 Communications Assistance for Law Enforcement Act (CALEA) established legal requirements for telecommunications operators in the US, while technical protocols were enacted across Europe under the auspices of the European Telecommunications Standards Institute (ETSI).[36] These standards have become known as Lawful Interception. In Russia, the System of Operative Investigative Measures (SORM) was put into practice in the early 1990s, which provides an architecture by which law enforcement and intelligence agencies can obtain direct access to data on commercial networks.[37] SORM-1, put into place in the early 1990s, allows for access to telephone and mobile networks. SORM-2, implemented in 1998, applies to IP traffic, and SORM-3 to interception of all communications media, providing quick access and long-term storage for a period of three years.[38]

Table 2 provides an overview of actors involved in a nationwide surveillance architecture.

Internet Service Providers (ISPs) and telecommunications operators, which manage networks and charge subscribers for certain services, such as internet, mobile and fixed-line telephony services, may be required to ensure that their networks are accessible to government agencies.

33 http://cryptome.org/jya/echelon-dc.htm

34 http://www.military.com/Content/MoreContent1/?file=cw_f_ivybells

35 See, for example, reports from the Church Committee on the formation, operation, and abuses of U.S. intelligence agencies http://www.aarclibrary.org/publib/church/reports/contents.htm

36 Brown, I & Korff, D, "UK Information Commissioner Study Project: Privacy & Law Enforcement", Foundation for Information Policy Research, February 2004, p25, available at <http://discovery.ucl.ac.uk/3880/1/3880.pdf>

37 http://iks.sut.ru/publications/zakonnyy-perehvat-soobshcheniy-podhody-etsi-calea-i-sorm/

38 "Lawful interception: the Russian approach", Andrei Soldatov and Irina Borogan, Privacy International, 4 March 2013, available at https://www.privacyinternational.org/news/blog/lawful-interception-the-russian-approach

Telecommunications equipment vendors are companies which develop the necessary hardware, such as switches and routers, upon which networks run. Because they are developed with Lawful Interception capabilities, when they are exported some equipment by default actively carries out surveillance, or is designed in a way to be easily accessible for surveillance purposes. Some vendors specially develop and market equipment for surveillance purposes.

Surveillance companies sell technologies for law enforcement and intelligence purposes. These can be systems which facilitate the Lawful Interception process, sold for example to operators for compliance purposes, or sold directly to government agencies providing more widescale, untargeted, and intrusive capabilities.

Industry actors involved in surveillance architecture

Actor	Technology/Services	Example
ISPs/Telecommunications Operator	Internet and telephone services. Either government-owned or private with diverse shareholders	AT&T, Vodafone, Comcast, Orange, Telecom Egypt, Uzbektelecom
Submarine cable providers	Submarine cable operators / Landing points operators. Generally financed by consortia of operators	TATA-3, China Unicom, Hibernia, Level 3, Atlantic Crossing, Huawei Marine
Telecommunications Network Equipment Vendors	Standard network nodes such as switches and gateways, some of which are designed to be capable of interception, or designed for network monitoring	Ericsson, Nokia, Huawei, ZTE, Cisco, Bluecoat
Surveillance companies	Surveillance technologies sold exclusively to government agencies or telecommunications companies for government purposes	Verint, NICE Systems, Qosmos, Trovicor, Hacking Team, NeoSoft, VasTech, Palantir
Contractors & PMSCs	Consulting and staff	Booz Allen Hamilton, BAE, SAIC, Chertoff Group, ManTech
Distributors	Partners and resellers of surveillance technologies	Elamen, Ezzy Group

The Privacy International SII consists of surveillance companies, the more high profile and distributors specialising in surveillance technologies, and some telecommunications network equipment vendors.

Graphs 1, 2 and 3 show the geographical distribution of the companies in the SII, when they were created, and the types of surveillance technology.

THE SURVEILLANCE INDUSTRY IN THE WORLD

We have gathered data on **528** companies in the surveillance industry.

The top 5 HQ countries are **United States of America** (122 companies), **United Kingdom** (104), **France** (45), **Germany** (41) and **Israel** (27).

510 companies are located in the northern hemisphere, while only **18** can be found in the southern hemisphere.

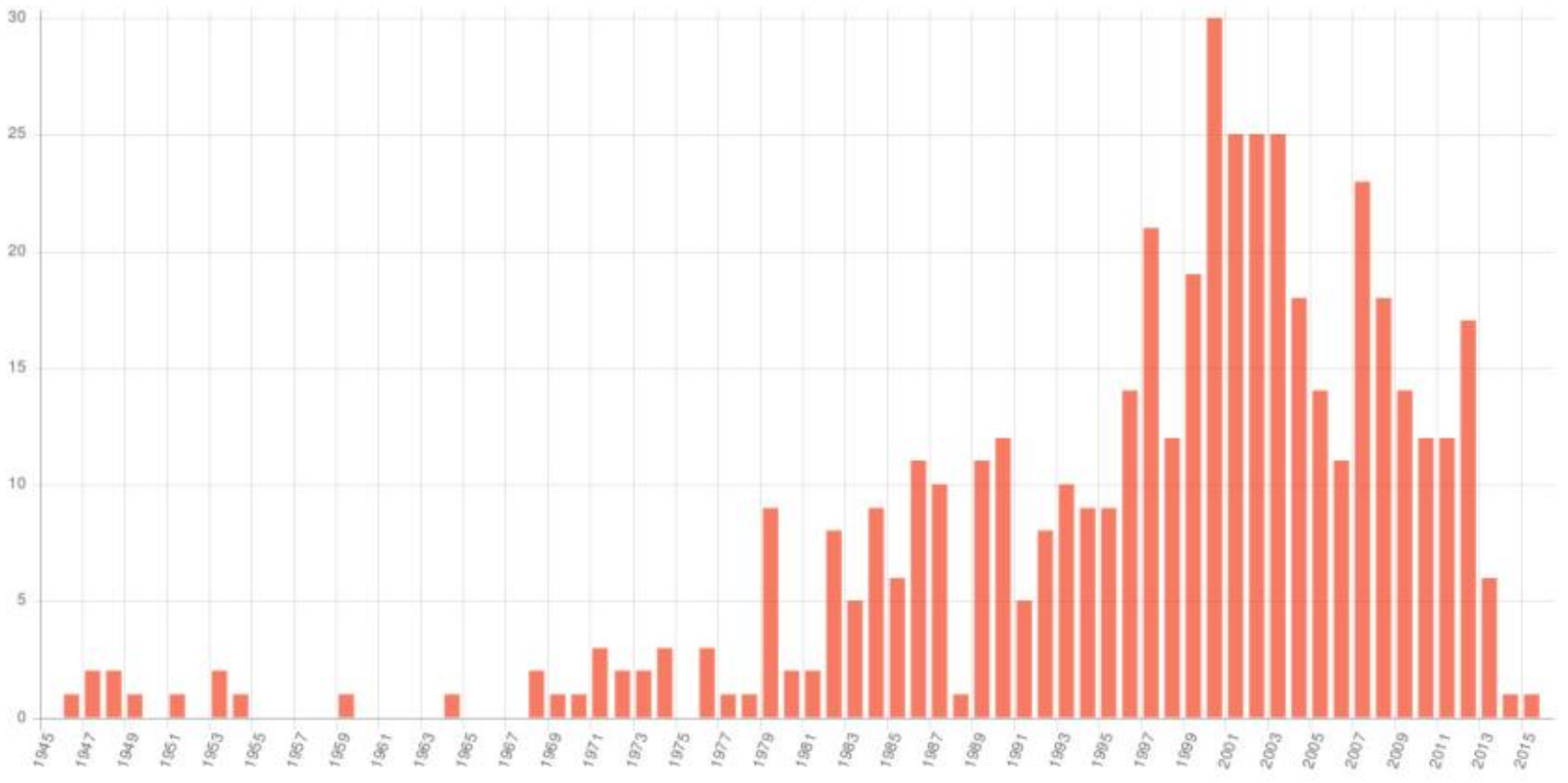
75% of the companies belong to **NATO** countries.

87% are based in **OECD** member countries.

4% rank in the top 100 largest arms-producing and military services companies in the world.

88% have their HQ in a country that participates in the **Wassenaar Arrangement**.

HOW MANY SURVEILLANCE COMPANIES ARE CREATED EACH YEAR



THE SURVEILLANCE INDUSTRY IN THE EU

Out of the **28** EU countries, we've identified **23** where we can find surveillance companies.

The top 5 HQ countries in the EU are **United Kingdom** (104 companies), **France** (45), **Germany** (41), **Italy** (18) and **Sweden** (9).

The top 5 HQ cities are **London** (15), **Paris** (13), **Stockholm** (6), **Dublin** (5) and **Munich** (5).

COUNTRY DISTRIBUTION OF SURVEILLANCE COMPANIES

THE TYPES OF SURVEILLANCE TECHNOLOGY

ANALYSIS
Use data to map relationships, recognise patterns, and analyse words' meaning

Example: Relationship mapping software

AUDIO SURVEILLANCE
Record and transmit audio

Example: Speaker identification software which compares recordings against target voice samples

VIDEO SURVEILLANCE
Use video cameras

Example: Wide Area Persistant Surveillance systems

PHONE MONITORING
Gather data communicated across mobile, fixed or next generation networks

Example: IMSI catchers

LOCATION MONITORING
Monitor the location of a target using phone identifiers or tracking devices

Example: GPS tracking devices

INTERNET MONITORING
Technologies that gather information communicated across the internet

Example: Optical Fiber Cable taps

MONITORING CENTRE
Combine different surveillance technologies (internet, phone etc) into one suite

Example: Monitoring Centres offered by surveillance companies

INTRUSION
Remotely installed on communication devices to extract data & control functions

Example: Commercial "spyware"

BIOMETRICS
Identify individuals on distinctive physiological or behavioral characteristics

Example: Facial recognition software

COUNTER-SURVEILLANCE
Detect and counter surveillance

Bug detection tools

EQUIPMENT
Aids the operation of surveillance and counter surveillance capabilities

Example: Vans or vehicles in which surveillance technology can be installed

FORENSICS
When attached to a device, extract and visualise data from it

Example: Commercial software packages offered by surveillance companies

COMPANIES PER TECH TYPE

The Wassenaar Arrangement

International export control regimes, legacies of cooperation on the trade in strategically sensitive goods from the Cold War, act as forums in which states decide which specific items should be subject to licensing. Currently, there are separate international forums concentrating on missile technology, chemical, biological, nuclear, and military goods. The Wassenaar Arrangement stipulates which military and "dual-use" goods should be subject to licensing and has 41 participating states, including Russia, Japan, the US, and the EU member states. Dual-use goods are generally those which have both military and civilian use, meaning that the arrangement does not include items purely because of human rights concerns. Nevertheless, the Wassenaar Arrangement includes several surveillance technologies within its dual use list of controlled items. While there are only 41 offically participating states, the list of items are also used by a large number of other states as part of their own licensing regulations, including Israel and, to an extent, China.[39]

Companies in the SII are overwhelmingly based in large arms exporting countries. Four of the top 5 countries in the SII where companies are headquartered also rank in SIPRI's top five arms exporting countries over the years 2000-2015 (USA, Germany, UK, France). 17 of the top 20 countries in which companies in the SII are headquartered also rank within SIPRI's top twenty arms exporting countries during that period.[40]

Using UK government figures, eight of the top 10 countries in the SII where companies are based also rank in the top ten defence exporters over the years 2005-2014.

Estimated Top Defence Exporters (Based on Orders/Contracts signed): 2005-14 ($BN)

Source: United Kingdom Trade & Investment Defence & Security Organisation[41]

Exporting Country	US$BN	Exporting Country	US$BN
USA	204	Canada	17
UK	116	Italy	16
Russia	73	Sweden	13
France	57	Spain	12
Germany	21	Republic of Korea	8
Israel	18	Turkey	6

39 https://www.gov.uk/government/publications/analysis-of-chinas-export-controls-against-international-standards/bridging-the-gap-analysis-of-chinas-export-controls-against-international-standards

40 Figures taken from SIPRI Arms Transfers Database, available at: <http://www.sipri.org/databases/armstransfers>. Largest exporters (In descending order in SIPRI Trend Indicator Values (TIVs) expressed in US$ m. at constant (1990) prices): United States, Russia, Germany (FRG), France, United Kingdom, China, Italy, Spain, Israel, Netherlands, Ukraine, Sweden, Switzerland, Canada, South Korea, Norway, Belarus, South Africa, Turkey, Poland

41 https://www.gov.uk/government/statistics/uk-defence-and-security-export-figures-2013

There is also a high level of overlap with large arms exporters within the EU, with 7 of the top 10 countries in the SII where companies are headquartered in the EU also featuring in SIPRI's top ten EU defence exporters over the years 2000-2015.[42]

They are also overwhelmingly based in advanced capitalist economies, with 87% of the 528 companies based in Organisation for Economic Co-operation and Development (OECD) states.

Of the 528 companies, 75% have their headquarters within North Atlantic Treaty Organization (NATO) states.

4% of companies which feature in the SII also feature in the SIPRI top 100 arms producing companies of 2014[43] including US-based Boeing (ranked 2nd) BAE Systems, based in the United Kingdom (ranked 3rd), and Elbit Systems, based in Israel (ranked 33rd).

42 Figures taken from SIPRI Arms Transfers Database, available at: <http://www.sipri.org/databases/armstransfers>. Largest exporters (In descending order in SIPRI Trend Indicator Values (TIVs) expressed in US$ m. at constant (1990) prices): Germany (FRG), France, United Kingdom, Italy, Spain, Netherlands, Sweden, Poland, Belgium, Finland

43 http://www.sipri.org/research/armaments/production/recent-trends-in-arms-industry/The%20SIPRI%20Top%20100%202014.pdf

Selected Case Studies[44]

Israel

Exports of military and security equipment serve a dual purpose in Israel.[45] Firstly, a commercial one, providing companies and individual brokers with revenues that are then reinvested into the industrial base, ultimately to the benefit of Israeli military and security agencies. Secondly, exports foster military, security, and diplomatic ties with recipient countries. Exports of intelligence equipment can play a particularly important role in strengthening intelligence cooperation. It is unclear how high a priority is placed on the consideration of human rights within decision making in Israel's government when it comes to licensing exports of strategic goods. A recent amendment to export licensing rules that would have put the consideration of human rights records into law was rejected by the foreign ministry.[46] Activists have pointed to ongoing military exports from Israel to Azerbaijan and South Sudan as evidence that military exports from Israel are leading to human rights violations.[47]

Military conscription is mandatory in Israel, meaning that the entire non-Arab population with some exceptions receives military or intelligence training. In addition to intelligence units of the armed forces and the domestic and foreign intelligence agencies, the signals intelligence agency responsible for monitoring communications, known as Unit 8200, is the largest unit within the Israeli Defense Forces.[48] In 2014, 43 former Unit 8200 soldiers issued a letter to the Prime Minister saying that there was no oversight on surveillance methods used by the unit against Palestinians, allowing "for the continued control of millions of people and in-depth inspection that's invasive to most areas of life".[49] Expertise learned during military and intelligence service can then be applied to the private sector. The Financial Times reports that Israeli companies account for some 10% of the global cyber security market, and that in 2014 exports of cyber security equipment exceeded exports of military hardware for the first time.[50]

There are 27 surveillance companies with headquarters in Israel in the SII. Out of the top five countries represented in SII, Israel is home to by far the largest amount per capita, with 0.33 companies per 100,000 people located in Israel, compared to 0.04 in the United States and 0.16 in the United Kingdom.

---

44 Chosen as the top 5 countries in which surveillance companies are based, but with Italy replacing France due to their being more information available in the public domain on transfers from Italy to inform analysis

45 http://www.globes.co.il/en/article-1000635747

46 http://972mag.com/who-will-stop-the-flow-of-israeli-arms-to-dictatorships/114080/

47 http://www.haaretz.com/israel-news/.premium-1.669852

48 http://www.haaretz.com/israel-news/.premium-1.585863

49 http://www.ynetnews.com/articles/0,7340,L-4570256,00.html

50 http://www.ft.com/cms/s/2/69f150da-25b8-11e5-bd83-71cb60e8f08c.html

Investigations published by Privacy International show that Israeli companies have provided phone and internet monitoring technologies to the secret police in Uzbekistan and Kazakhstan,[51] as well as security forces in Colombia.[52] Other reports detail Israeli surveillance companies have equipped security forces with internet monitoring technology in Trinidad and Tobago[53] and Uganda.[54] Agencies in Panama and Mexico have reportedly been customers of intrusion technology developed by Israeli NSO Group.

Israeli brokers likely amplify Israel's role in the military and security trade,[57] also meaning that Israeli companies are likely under-represented in the SII. Some muslim-majority countries, such as Saudi Arabia and Bangladesh, explicitly ban Israeli companies from competing in some procurement.[58] A freedom of information request confirmed that by 2012 there were 6684 registered arms brokers in Israel, working in 1006 companies and 312 independent businesses.[59] This makes enforcing regulations in Israel challenging, and indeed the agency in charge of supervising strategic exports has been criticized by a state comptroller for weak enforcement.[60] Internet monitoring technology sold by Allot Communications has reportedly even been re-exported to Iran.[61] Israeli brokers are reported to have arranged transfers of internet and phone monitoring equipment to Nigeria,[62] while surveillance companies such as Circles, registered in Cyprus and Bulgaria,[63] and 3i-Mind,[64] registered in Switzerland, are staffed by former employees of Israeli surveillance companies and intelligence agencies. Silver Bullets, a UK based company reported to have supplied phone monitoring technology to Vietnam,[65] has an Israeli national as a registered officer.[66]

51 'Private Interests: Monitoring Central Asia', Privacy International, Nov. 2014

52 'Demand/Supply: Exposing the Surveillance Industry in Colombia', Privacy International, September 2015, https://www.privacyinternational.org/sites/default/files/DemandSupply_English.pdf>

53 "'Phone calls, e-mails of high-profile citizens monitored for past two years'", Daily Express, 26 November 2008, <http://www.trinidadexpress.com/news/Listening_in___-115542299.html>

54 Africa Intelligence,"Museveni commits $85.5 million to monitor the Web", N°1414 - 06/11/2015 <http://www.africaintelligence.com/ION/politics-power/2015/11/06/museveni-commits-dollars85.5%C2%A0million-to-monitor-the-web,108110202-ART>

55 Bamford, James, "The Espionage Economy", Foreign Policy, 22 January 2016, http://foreignpolicy.com/2016/01/22/the-espionage-econom>

56 Barbara Opall-Rome, 'Israeli Smartphone Targeting System Cleared for Export', Defense News, Aug. 2013

57 http://www.nonproliferation.eu/web/documents/other/siemontwezeman4f7dafb3c4a92.pdf

58 https://wikileaks.org/saudi-cables/doc43348.html

59 http://www.haaretz.com/israel-news/.premium-1.535794

60 http://www.upi.com/Business_News/Security-Industry/2013/07/19/Israeli-defense-industry-exports-under-scrutiny/UPI-11581374259134/

61 http://www.globes.co.il/en/article-1000718874

62 http://www.premiumtimesng.com/investigationspecial-reports/196964-how-jonathan-govt-paid-companies-linked-to-doyin-okupe-to-hack-unfriendly-websitesinvestigation-how-jonathan-govt-paid-companies-linked-to-doyin-okupe-to-hack-unfriendly-websites-2.html

63 http://www.intelligenceonline.com/corporate-intelligence/terabytes/2015/12/02/circles--mobile-phone-company-intercepts-3g,108114286-ART

64 http://www.forbes.com/sites/jeffbercovici/2013/10/31/vocativ-brings-the-tools-of-the-spy-world-into-the-newsroom/#4eac16857a17

65 http://boingboing.net/2006/08/24/report-uk-us-cos-sol.html

66 https://beta.companieshouse.gov.uk/company/04338196/officers

SURVEILLANCE TRANSACTIONS IN ISRAEL

REPORTED TRANSFERS

INTRUSION SOFTWARE	Mexico Panama
LAWFUL INTERCEPTION	Kazakhstan Uganda Uzbekistan
DEEP PACKET INSPECTION	Iran Kazakhstan Uzbekistan
MONITORING CENTRE	Kazakhstan Nigeria Uganda Uzbekistan
FIBRE TAPS/PROBES	Colombia Nigeria

ISRAEL

COMPANIES BASED IN ISRAEL

Ability Cellebrite Checkpoint Software Cyberbit Elbit Elkat
Elta Systems Gita Technologies KeySee Software Magen MER Group
Natural Speech Communication
Netline Communications Technologies (NCT) Nice Systems NSO Group
Phantom Technologies Picsix Rayzone Group Septier Silicom
Tadiran Electronic Systems Tar Ideal Concepts Terrogence TraceSpan
Unipier Wintego Wirex

TECHNOLOGY TYPE DISTRIBUTION

United States of America

There are 122 companies with headquarters in the United States – the most in the SII. One of the most obvious explanations for this would be the relative size and sophistication of security agencies within the US and size of the domestic US market for surveillance technology. The 'Black Budget',[67] a leaked breakdown of expenditure of the 2013 US intelligence program, which does not include amounts for law enforcement agencies such as the Drug Enforcement Administration, revealed that the total US intelligence budget in 2013 was $52.6 billion - in constant dollars estimated to be double that of 2001. According to a Bloomberg Industries analysis, 70% of the 2013 United States intelligence budget was contracted out to private companies,[68] while the 'Black Budget' revealed that over 20% of 107,035 employees across the various intelligence agencies were private contractors.[69] Research and development into high technology are subsidised through the Pentagon and subsequently commercialised.[70] Total US military expenditure – including R&D - was in 2015 at $596 billion, more than double that of second-placed China, and 36% of the global share of expenditure.[71]

Internet and phone monitoring technology developed by Narus, a former subsidiary of Boeing until it was baught over by Symantec, a fortune 500 technology company, has been used to monitor the AT&T network by the NSA.[72] According to their marketing vice president, Narus' technology is a capable of recording all traffic in an internet protocol network, including emails, attachments, internet histories, and even VoIP calls. It was reportedly also used in Egypt prior to the 2011 uprising.[73]

67 https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html

68 http://www.bloomberg.com/news/articles/2013-06-20/booz-allen-the-worlds-most-profitable-spy-organization

69 https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-

70 Understanding Power: The Indispensible Chomsky By Noam Chomsky, p 241

71 http://books.sipri.org/files/FS/SIPRIFS1604.pdf

72 Markoff, J and Shane, S, "Documents Show Link Between AT&T and Agency in Eavesdropping Case," The New York Times, 13 April 2006, <http://www.nytimes.com/2006/04/13/us/nationalspecial3/13nsa.html?_r=2&n=Top/News/Business/Companies/AT&T&oref=slogin&>

73 Karr, Timothy, "One U.S. Corporation's Role in Egypt's Brutal Crackdown," Huffington Post, 28 Janury 2011, http://www.huffingtonpost.com/timothy-karr/one-us-corporations-role-_b_815281.html>

Privacy International has also found within public US government procurement records that surveillance companies Packet Forensics and SS8 are selling to a range of US government agencies as well as exporting surveillance equipment abroad.[74] [75] SS8 were also reportedly responsible for selling intrusion systems to the United Arab Emirates.[76] Data about the use of products developed by Blue Coat, which produces Deep Packet Inspection technology that can be used for internet monitoring, was compiled by the Citizen Lab.[77] The Intercept reports that Lawful Interception companies, without naming any specific companies, have apparently provided the NSA with direct access to foreign telecommunications networks.[78] Other exports by US companies include Colombia, where there are high levels of US security assistance and intelligence cooperation.[79]

74 "List Of Contract Actions Matching Your Criteria: SS8", Federal Procurement Data System, 3 February 2016 https://www.fpds.gov/ezsearch/search.do?indexName=awardfull&templateName=1.4.4&s=FPDSNG.COM&q=ss8>

75 "List Of Contract Actions Matching Your Criteria: Packet Forensics", Federal Procurement Data System, 3 February 2016 <https://www.fpds.gov/ezsearch/search.do?indexName=awardfull&templateName=1.4.4&s=FPDSNG.COM&q=packet+forensics>

76 http://news.bbc.co.uk/1/hi/8161190.stm

77 Citizen Lab, "Some Devices Wander by Mistake: Planet Blue Coat Redux," 09 July 2013, <https://citizenlab.org/2013/07/planet-blue-coat-redux/>

78 https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

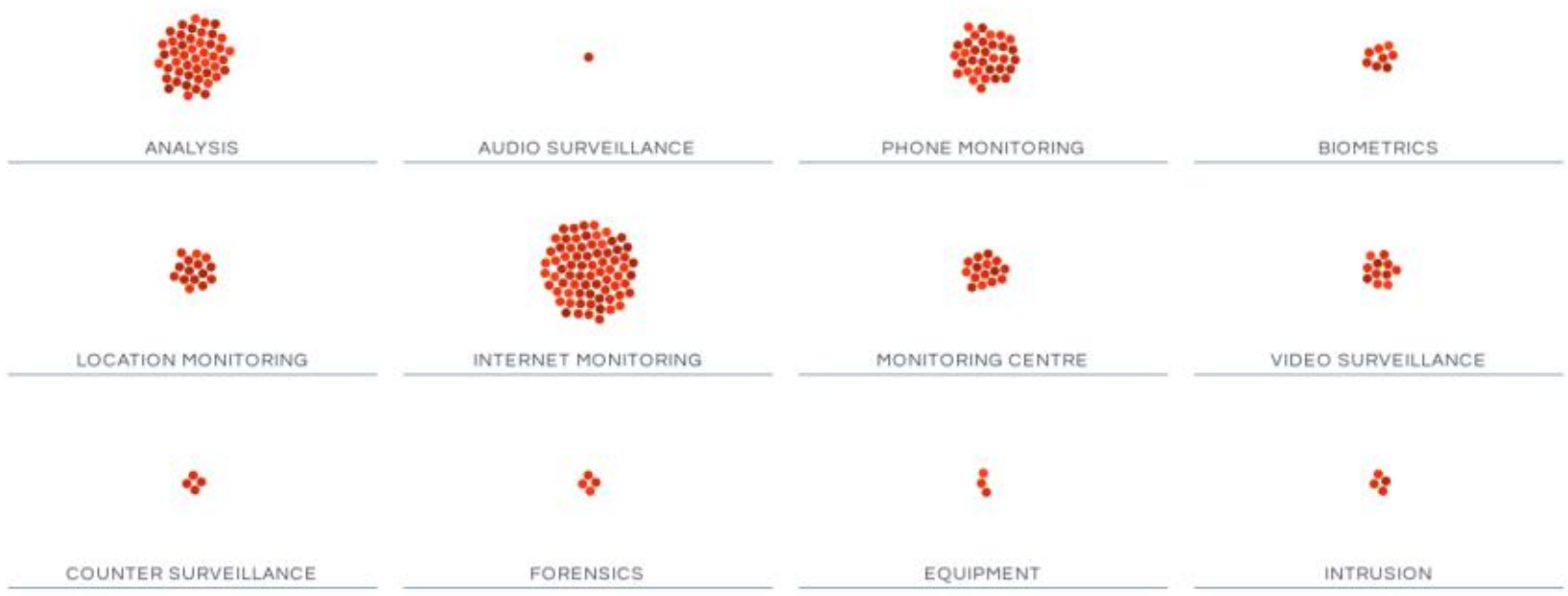
79 'Demand/Supply: Exposing the Surveillance Industry in Colombia', Privacy International, September 2015, https://www.privacyinternational.org/sites/default/files/DemandSupply_English.pdf>

THE UNITED STATES OF AMERICA

COMPANIES BASED IN THE USA

Access Data Acme Packet Adax AGI AirMagnet Almenta Amdocs
Andrew Network Solutions ATCI Basis Technology
Berkeley Varitronics Systems Bivio Blue Coat Brightplanet Broadsoft
Brocade Calient Cellular Data Resources Chenega Corporation
Chenega Federal Systems Cisco Systems Cloudshield Technologies
Cogent Comverse CSC Cubic Cyveillance Defentek Dialogic
ELSAG EMC Empirix Endgame Systems Exelis
Federal Signal Technologies FireEye Freight Watch Frontline
Garland Technology General Dynamics Geofeedia Gigamon
GL Communications Glimmerglass Guidance Software Harris
Hewlett-Packard Hexis Cyber Solutions i2 Image Sensing Systems
Ineoquest Technologies Intelligentias IP Fabrics Kapow Software
Kingfisher Systems L-3 Linkabit Lockheed Martin Loquendo
Mandiant Mantaro ManTech Meganet Narus Net App Net Optics
Netezza NetQuest Netronome Networks NetScout Systems
NetWitness Network Instruments Neustar Newport Networks
Niksun Northrop Grumman Ntrepid Nuance Technology Objectivity
Onpath Technologies Oxygen Forensics Packet Forensics Palantir
Paraben Passware Pen Link Phoenix Polaris Wireless Procera
PV Labs Radisys Radware Raytheon Retentia SAIC Salient Stills
SAS Institue Inc Savvius SenSage SevOne Simena SnapTrends
Solera Networks Sonus Networks SS8 Networks Subsentio
Teel Technologies TeleStrategies Tilera Corporation TruePosition
Ultra Electronics Advanced Tactical Systems Ultrareach Verint
View Systems Visual Analytics Vocal Technologies VSS Monitoring
WCCTV Wildpackets XALTED Yaana Nuix
Research Electronics International

TECHNOLOGY TYPE DISTRIBUTION



SURVEILLANCE TRANSACTIONS IN THE USA

REPORTED TRANSFERS

INTRUSION SOFTWARE
United Arab Emirates

LAWFUL INTERCEPTION
Colombia India Kazakhstan Mexico Pakistan Suriname Switzerland Trinidad and Tobago United States of America Uzbekistan

NETWORK INFRASTRUCTURE AND SERVICES
China Colombia Kazakhstan

OFF THE AIR INTERCEPTION
Afghanistan Bosnia and Herzegovina Colombia Denmark Dominican Republic Egypt El Salvador Germany Iraq Israel Jordan Lebanon Mexico Netherlands Nigeria Pakistan Peru Syria Turkey United Kingdom United States of America Uruguay

MONITORING CENTRE
Colombia Kazakhstan Mexico Switzerland Trinidad and Tobago Uzbekistan

DEEP PACKET INSPECTION
Afghanistan Argentina Austria Bahrain Bangladesh Belgium Bermuda Bolivia Brazil Brunei Cameroon Canada Chile China Colombia Costa Rica Côte d'Ivoire Democratic Republic of Congo Denmark Dominican Republic Ecuador Egypt Finland France Gambia Georgia Germany Guatemala Guyana Hong Kong India Indonesia Iran Iraq Israel Italy Jamaica Japan Jordan Kazakhstan Kenya Kuwait Lebanon Malaysia Maldives Mauritius Mexico Monaco Netherlands Nicaragua Nigeria Norway Pakistan Palestine Panama Peru Philippines Portugal Qatar Russia Rwanda Saudi Arabia Seychelles Singapore Slovakia Solomon Islands South Africa South Korea Spain Sri Lanka Sudan Swaziland Sweden Switzerland Syria Taiwan Tanzania Thailand Turkey Uganda United Arab Emirates United Kingdom United States of America Uzbekistan Venezuela Zambia

FIBRE TAPS/PROBES
Colombia United States of America

NETWORK INFRASTRUCTURE
Syria

United Kingdom

Largely spurred by the conflict in Northern Ireland, the United Kingdom was already by 1981 becoming a world-leader in the development of surveillance and counter-insurgency technology.[80] There are 104 UK companies in the SII. Currently, general UK cyber capabilities are spurred by the sophistication of its signals intelligence agency, the Government Communications Headquarters (GCHQ), and the fact it is home to a number of large arms companies.[81]

The UK government also promotes exports abroad through the UK Trade and Investment Defence and Security Organisation, for example proactively assisting surveillance company Hidden Technologies to access markets abroad by providing advice and introducing the company to potential customers.[82] BAE Systems in 2011 acquired Danish internet and phone monitoring company ETI for £137 million.[83] Bloomberg reports that since 2008, BAE has spent more than £1 billion on buying surveillance and cyber-security businesses.[84] Little is known of BAE's exports however, other than it has been reported that ETI had provided the Tunisian government with internet monitoring technology prior to the 2011 uprising,[85] and that it was the "main contractor" and "systems integrator" for a project in Saudi Arabia.[86]

The UK government has since 2015 made export licensing data publicly available. 98 permanent and temporary licenses were granted in the period 1 January – 31 December 2015 for phone monitoring technology, including to Israel, Bangladesh, Egypt, Saudi Arabia, Turkmenistan, and the UAE.[87] Exports of phone monitoring technology (IMSI catchers, see technology explainer in annex 1) have been blocked on human rights ground to a country in South Asia[88] in 2009 and to Ethiopia and Pakistan in 2015. An Open Individual Export License (OIEL) was granted for equipment, software, and technology for Intrusion Software on 14 October 2015, giving an exporter permission to sell to 11 countries, including Egypt, Qatar, Saudi Arabia, and the United Arab Emirates. A license worth £6.5m was issued by the UK on 7 July 2015 for internet monitoring technology to the UAE. It is not known whether the licenses for internet monitoring and intrusion are for law enforcement/intelligence gathering purposes.

80 https://www.amnesty.org/download/Documents/200000/pol340051981en.pdf

81 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275566/UKTI_Cyber_Security_Brochure.pdf

82 https://www.gov.uk/government/case-studies/technology-company-helped-to-secure-millions-of-pounds-of-export-business

83 http://www.computing.co.uk/ctg/news/2074597/bae-systems-buys-cyber-security-firm-gbp137m

84 http://www.bloomberg.com/news/articles/2016-04-12/bae-taps-cyber-skills-honed-for-spooks-to-win-corporate-clients

85 http://www.bloomberg.com/news/articles/2011-12-12/tunisia-after-revolt-can-alter-e-mails-with-big-brother-software

86 https://www.information.dk/indland/2016/04/dansk-firma-samarbejde-saudi-arabien-overvaagning

87 UK Department for Business Innovation and Skills, 'Strategic export controls: reports and statistics', <https://www.exportcontroldb.bis.gov.uk>.

88 http://www.cecimo.eu/site/fileadmin/documents/EU%20LEGISLATION%20AND%20DOSSIERS/Dual-use_legislation/FINAL_REPORT.pdf

THE UNITED KINGDOM

COMPANIES BASED IN THE UK

Rinicom Ltd 360 Vision A.i. Solve Aappro ABM Aculab
Advanced Research and Technology Allevate Ansec IA Arithmetica
AST-Systems Audiotel International Aurora Autonomy BAE Systems
BCB International Blighter Surveillance Systems Cambridge Consultants
Cambridge Intelligence CarroGWP Cellxion Chronos Technology
Clearswift Clues Cobham CommsAudit Comstrac CopperEye
Cosworth Creativity Software CRFS Datong
David Horn Communications Delma MSS Detica Digital Barriers
DigitalRF Electrosonic Erebus Eskan Evidence Talks Facebanx
FMS Group Forensic Pathways Forensic Telecommunications Services
Futurum Consultancy & Training Gamma Group Global Forensics
Griff Comm Hidden Technology Systems International
Human Recognition Systems IPL Kirintec Komcept Solutions
L-3 ASA L-3 TRL Technology Lateo Surveillance MASS MCM Solutions
Megablue Technologies Metaswitch MGT Europe
NDI Recognition Systems Net X Solutions Network Critical
News Datacom Research OmniPerception One Digital Panoptech
Pda Electronics QCC Radio Tactics RFEL Roke Manor Research
Secure Information Assurance Security Research Selex ES
Shield Security Silver Bullets Smith Myers Smoothwall
Sonic Communications Sonicwall Sophos Speedog
Spirent Communications Sure SystemWare Europe
Telesoft Technologies Terrafix ThorpeGlen Torchlight
Total Secure Automation Ultra Electronics Network Analytics
United Advanced Technologies International Vislink Group Winkelmann
Wynyard Group XAD Communications Qinetiq GOS Systems
Seven Technologies Group Providence itf Kelvin Hughes

TECHNOLOGY TYPE DISTRIBUTION

ANALYSIS

AUDIO SURVEILLANCE

PHONE MONITORING

BIOMETRICS

LOCATION MONITORING

INTERNET MONITORING

MONITORING CENTRE

VIDEO SURVEILLANCE

COUNTER SURVEILLANCE

FORENSICS

EQUIPMENT

INTRUSION

SURVEILLANCE TRANSACTIONS IN THE UK

REPORTED TRANSFERS

INTRUSION SOFTWARE

Angola, Australia, Austria, Bahrain, Bangladesh, Belgium, Bosnia and Herzegovina, Brunei, Bulgaria, Canada, Czech Republic, Egypt, Estonia, Ethiopia, Gabon, Germany, Hungary, India, Indonesia, Italy, Japan, Jordan, Kazakhstan, Kenya, Kuwait, Latvia, Lebanon, Lithuania, Macedonia, Malaysia, Mexico, Mongolia, Morocco, Netherlands, Nigeria, Oman, Pakistan, Panama, Paraguay, Philippines, Qatar, Romania, Saudi Arabia, Serbia, Singapore, Slovenia, South Africa, Spain, Taiwan, Turkey, Turkmenistan, Uganda, United Arab Emirates, United Kingdom, United States of America, Venezuela, Vietnam

LAWFUL INTERCEPTION

Oman

OFF THE AIR INTERCEPTION

Algeria, Bangladesh, Brazil, Brunei, Cambodia, Chile, China, Colombia, Egypt, El Salvador, Ethiopia, Hong Kong, India, Indonesia, Iraq, Israel, Kuwait, Lebanon, Macao, Macedonia, Malaysia, Namibia, Oman, Pakistan, Paraguay, Philippines, Qatar, Saudi Arabia, Singapore, South Africa, South Korea, Sri Lanka, Taiwan, Thailand, Tunisia, Turkey, Turkmenistan, United Arab Emirates, Vietnam

DEEP PACKET INSPECTION

United Arab Emirates

LOCATION TRACKING

Iran

FIBRE TAPS/PROBES

Colombia, United Arab Emirates

Germany

There are 41 German companies in the SII. Germany is a world-renowned leader in high-tech manufacturing, driven by public-private research.[89] It is also Europe's largest arms exporter and during the Cold War home to intelligence agencies notoriously active in espionage and monitoring of civilian populations.[90]

Publicly available reports show German companies exporting a range of phone and internet monitoring technologies to Bahrain,[91] Bangladesh,[92] Iran,[93] and Syria,[94] among others. Privacy International has reported how German companies have been involved in the sale of such technology to Ethiopia[95] and Pakistan.[96] In 2014, the government conducted a review of exports of surveillance technology, reporting that undisclosed surveillance technology had been exported to 38 countries between 2003 and 2013, including to Saudi Arabia and Turkmenistan.[97]

89 http://www.wsj.com/articles/behind-germanys-success-story-in-manufacturing-1401473946

90 http://www.spiegel.de/international/germany/cold-war-espionage-10-000-east-germans-spied-for-the-west-a-508518.html

91 Silver, V. And Elgin, B., 'Torture in Bahrain becomes routine with help of Nokia Siemens', Bloomberg, 23 Aug. 2011, <http://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking>, Silver, V., 'EU may probe Bahrain spy gear abuses', Bloomberg, 24 Aug. 2011, <http://www.bloomberg.com/news/articles/2011-08-24/eu-legislators-ask-for-inquiry-into-spy-gear-abuses-in-bahrain>

92 Spohr, Frederic, "Big Brother Made in Germany", Handelsblatt, 27 March 2015, <https://global.handelsblatt.com/edition/145/ressort/politics/article/big-brother-made-in-germany>

93 Rhoads, C., 'Iran's web spying aided by Western technology', Wall Street Journal, 22 June 2009, <www.wsj.com/news/articles/SB124562668777335653#printMode>

94 Monitoring the opposition: Siemens allegedly sold surveillance gear to Syria', Der Spiegel, 11 Apr. 2012 <http://www.spiegel.de/international/business/ard-reports-siemens-sold-surveillance-technology-to-syria-a-826860.html>

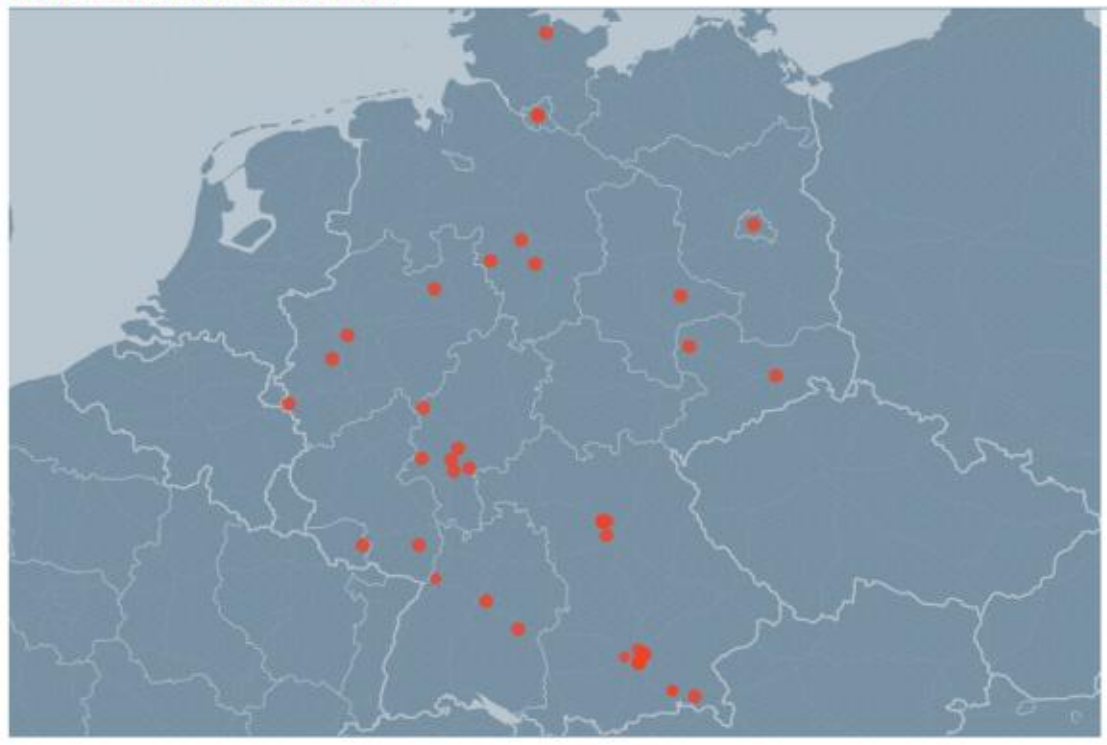
95 Privacy International, "Ethiopia expands surveillance capacity with German tech via Lebanon", 23 March 2015, <https://www.privacyinternational.org/node/546>

96 Privacy International, "Tipping the scales: Security & surveillance in Pakistan", July 2015, <https://www.privacyinternational.org/sites/default/files/PAKISTAN%20REPORT%20HIGH%20RES

97 German Parliament, Drucksache 18/2067 auf die Kleine Anfrage der Abgeordneten Agnieszka Brugger, Dr. Konstantin von Notz, Katja Keul, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN, 18.08.2014, Date accessed 03.02.2016, <http://dipbt.bundestag.de/dip21/btd/18/023/1802374.pdf>

GERMANY

COMPANIES BASED IN GERMANY



@one IT GmbH 3M Services Alarm ATIS Systems Avanoc Cassidian Cognitec Systems Datakom Desoma DigiTask DN Systems EBS Electronic Elaman FinFisher GTEN IBH Impex Ipoque IZT MEDAV mh Service GmbH MIB Electronic Pad Datentechnik Paessler PKi Electronic Intelligence Plath Rheinmetall Defence Rohde and Schwarz Schomandl SciEngines secunet Security Networks AG Selectronic Siemens SIM Secure Information Management Stordis Syborg Sympalog Trovicor Utimaco Vervis COMINT Services Wolf Intelligence Advanced German Technology

TECHNOLOGY TYPE DISTRIBUTION

ANALYSIS

AUDIO SURVEILLANCE

PHONE MONITORING

BIOMETRICS

LOCATION MONITORING

INTERNET MONITORING

MONITORING CENTRE

VIDEO SURVEILLANCE

COUNTER SURVEILLANCE

FORENSICS

EQUIPMENT

INTRUSION

SURVEILLANCE TRANSACTIONS IN GERMANY

REPORTED TRANSFERS

LAWFUL INTERCEPTION	Bahrain Ethiopia Iran Oman Pakistan Syria Tajikistan Tunisia
NETWORK INFRASTRUCTURE	Bahrain Iran Syria
UNKNOWN	Albania Argentina Chile India Indonesia Kosovo Kuwait Lebanon Malaysia Mexico Morocco Norway Oman Pakistan Qatar Russia Saudi Arabia Singapore Switzerland Taiwan Turkey Turkmenistan United Arab Emirates United States of America
MONITORING CENTRE	Bahrain Bangladesh Egypt Iran Pakistan Syria Tajikistan Tunisia Turkmenistan Yemen
FIBRE TAPS/PROBES	Ethiopia

Italy

There are 18 Italian companies featuring in the SII. In addition to having a large defence and security sector generally, the Italian surveillance industry has been driven by domestic demand as a result of organised crime, according to a surveillance company presentation in South Africa in 2014 attended by Privacy International.

Surveillance company AREA in 2009 began installing a monitoring centre in Syria before the Italian government took measures in 2011 to stop the project.[98] The government does not regularly publish export licensing data, meaning that all of the other data about Italian surveillance exports is related to Hacking Team, a developer and seller of intrusion technology based in Milan. Hacking Team has attracted the most attention among surveillance companies as a result of their internal systems being hacked in 2015 and subsequent revelations that they had exported to a range of authoritarian countries.[99] There are three other companies which market intrusion technology in Italy, and a range of other companies producing surveillance technologies.

98 Silver, V., 'Italian firm said to exit Syrian monitoring project', Bloomberg, 28 Nov. 2011, <http://www.bloomberg.com/news/2011-11-28/italian-firm-exits-syrian-monitoring-project-repubblica-says.html>

99 https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim

ITALY

COMPANIES BASED IN ITALY

Araknos Area BEA DIGINT Endoacustica
Expert System Semantic Intelligence Finmeccanica GR Sistemi
Hacking Team Innova IPS Midland RCS RESI Group Sio SpA
SPEI Spektra Vitrociset

TECHNOLOGY TYPE DISTRIBUTION

SURVEILLANCE TRANSACTIONS IN ITALY

REPORTED TRANSFERS

INTRUSION SOFTWARE

Azerbaijan Bahrain Brazil Chile Colombia Cyprus Czech Republic Ecuador Egypt Ethiopia Honduras Hungary Italy Kazakhstan Lebanon Luxembourg Malaysia Mexico Mongolia Morocco Nigeria Oman Panama Poland Russia Saudi Arabia Singapore South Korea Spain Sudan Switzerland Thailand Turkey United Arab Emirates United States of America Uzbekistan Vietnam

MONITORING CENTRE

Syria

Import Case Study: Middle East & North Africa (MENA)

The Arab Uprising threw attention to the security apparatus of the various countries in the MENA region, most of which were supported by Western states and were recipients of major defence and security exports, assistance, and intelligence cooperation.[100] The various agencies had access to a wide variety of surveillance technologies provided overwhelmingly by economically-advanced countries in the West. The SII currently contains data about 152 transfers to the region. Aside from China, from which companies have reportedly provided surveillance equipment to Iran[101] and Algeria,[102] South African VasTech, which had provided Ghadaffi's Libya with nationwide phone monitoring technology,[103] all of the transfers have been from member countries of the OECD. All of the transfers apart from those from China and Israel have also been from countries that are participating members of the Wassenaar Arrangement.

Specific surveillance technologies have reportedly been used for a range of human rights abuses in the region. In Bahrain, school administrator and human rights activist Abdul Ghani al Khanjar was tortured while being confronted with transcripts of his text messages and details of his personal communications – information reportedly gained by the use of phone monitoring technology developed in Germany.[104] Similarly, intrusion software developed in the UK was reportedly used to spy on some 77 Bahraini individuals, including prominent lawyers, activists and politicians.[105] Two judicial investigations are still underway in France relating to the complicity of companies selling internet surveillance technologies in torture and other human rights abuses in Libya and Syria after complaints taken by human rights NGOs FIDH and LDH.[106]

However, how specific technologies are used and their use in human rights violations is difficult to quantify given the levels of secrecy. For example, it is difficult to establish whether victims of extrajudicial killings or torture were initially identified or located using specific surveillance technologies, despite their obvious utility in this regard. Moreover, surveillance also has an intangible effect. Surveillance techniques

100 https://www.csis.org/analysis/changing-patterns-arms-imports-middle-east-and-north-africa

101 Stecklow, S, "Special Report: Chinese firm helps Iran spy on citizens", Reuters, 22 March 2012, <http://www.reuters.com/article/us-iran-telecoms-idUSBRE82L0B820120322>

102 Africa Intelligence, "Bouteflika set to be Internet spymaster", N°1176 ¬ 05/11/2015, <http://www.africaintelligence.com/MCE/power-brokers/2015/11/05/bouteflika-set-to-be-internet-spymaster,108109971-ART>

103 Sonne, P. and Coker, M., 'Firms aided Libyan spies', Wall Street Journal, <www.wsj.com/articles/SB10001424053111904199404576538721260166388>

104 http://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking

105 https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/

106 https://www.fidh.org/en/region/europe-central-asia/france/15116-france-opening-of-a-judicial-investigation-targeting-qosmos-for-complicity

which subject a population or significant component of a group to indiscriminate monitoring, which have been ruled an interference with the right to privacy by a number of courts,[107] also interfere with the freedom of expression and lead to self-censorship.[108] This has a particularly corrosive effect in countries with poor human rights records in the MENA region, and specifically on journalists, opposition movements, activists, and dissidents. Amnesty International in their annual 2015 reported that governments across the Middle East and North Africa region remained intolerant of criticism and dissent and curtailed rights to freedom of expression, association and peaceful assembly.[109] Freedom House, which carries out an annual assessment on political rights and civil liberties, ranked the Middle East and North Africa region as the worst in the world in 2015,[110] while the highest ranked MENA country in Reporters Without Borders' 2016 World Press Freedom Index was Tunisia – ranked 96th.[111]

107 http://curia.europa.eu/juris/documents.jsf?num=C-293/12#

108 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645

109 https://www.amnesty.org/en/latest/research/2016/02/annual-report-201516/

110 https://freedomhouse.org/report/freedom-world/freedom-world-2015#.VyoczpMrLeQ

111 https://rsf.org/en/ranking

SURVEILLANCE IMPORTS IN THE MIDDLE EAST AND NORTH AFRICA

ORIGIN	GOODS	CLIENT	DATE
BAHRAIN			
Germany	Network Infrastructure, Monitoring Centre, Lawful Interception	Government of Bahrain	2007
Germany	Network Infrastructure, Monitoring Centre, Lawful Interception	Government of Bahrain	mid-2000s
Germany	Monitoring Centre	Government of Bahrain	2009
USA	Deep Packet Inspection		
UK	Intrusion Software		2010
Italy	Intrusion Software	Midworld Barhein	2013
ISRAEL			
UK	Off the Air Interception		2015
UK	Off the Air Interception		2015
Switzerland	Off the Air Interception		2015
USA	Deep Packet Inspection		
USA	Off the Air Interception		2012
YEMEN			
Germany	Monitoring Centre		2009
IRAN			
Ireland	Network Infrastructure and Services	Irancell	2008
UK	Location Tracking	Irancell	2011
Sweden	Network Infrastructure and Services	Irancell	2009
Germany	Network Infrastructure, Monitoring Centre, Lawful Interception	Islamic Revolutionary Guard Corps	2008
Israel	Deep Packet Inspection	"Hossein", a technology distributor	2006
Germany	Network Infrastructure, Monitoring Centre, Lawful Interception	Â Islamic Revolutionary Guard Corps	2008
USA	Deep Packet Inspection		
China	Network Infrastructure and Services, Deep Packet Inspection, Lawful Interception	Telecommunications Co of Iran	2010
China	Network Infrastructure and Services, Deep Packet Inspection, Lawful Interception	MobinNet	2009
Germany	Lawful Interception	Islamic Revolutionary Guard Corps	
LIBYA			
South Africa	Monitoring Centre, Lawful Interception		
France	Monitoring Centre, Deep Packet Inspection, Lawful Interception, Fibre Probes		
ALGERIA			
UK	Off the Air Interception		2015
China	Lawful Interception		2010
UNITED ARAB EMIRATES			
UK	Off the Air Interception		2015
UK	Off the Air Interception		2015
UK	Off the Air Interception		2015
UK	Off the Air Interception		2015
UK	Deep Packet Inspection, Fibre Probes		2015
UK	Intrusion Software		2015
Switzerland	Off the Air Interception		2012
Switzerland	Off the Air Interception		2013
Germany	Unknown		2011
Germany	Unknown		2006
Germany	Unknown		2003
USA	Deep Packet Inspection		
Italy	Intrusion Software	UAE - MOI	2011
Italy	Intrusion Software	UAE - Intelligence	2012
USA	Intrusion Software		2009
UK	Off the Air Interception		2015
UK	Intrusion Software		

EGYPT

Germany	Monitoring Centre		2009
UK	Intrusion Software	Technology Research Department (TRD)	
UK	Off the Air Interception		2015
UK	Intrusion Software		2015
USA	Deep Packet Inspection		
	Deep Packet Inspection	Ministry of Interior	2014
Italy	Intrusion Software	Egypt - MOD	2011
Italy	Intrusion Software	Egypt TRD GNSE	2015
USA	Off the Air Interception		2007

KUWAIT

UK	Off the Air Interception		2015
UK	Intrusion Software		2015
Switzerland	Off the Air Interception		2015
Switzerland	Off the Air Interception		2015
Finland	Off the Air Interception		2014
Finland	Off the Air Interception		2014
Germany	Unknown		2012
Germany	Unknown		2008
USA	Deep Packet Inspection		
Switzerland	Off the Air Interception		2016
UK	Off the Air Interception		2015

LEBANON

UK	Intrusion Software	General Directorate of General Security Internal Security Forces (ISF)	
UK	Off the Air Interception		2015
UK	Off the Air Interception		2015
Switzerland	Off the Air Interception		2012
Switzerland	Off the Air Interception		2012
Switzerland	Off the Air Interception		2013
Switzerland	Off the Air Interception		2013
Switzerland	Off the Air Interception		2014
Switzerland	Off the Air Interception		2015
Germany	Unknown		2011
USA	Deep Packet Inspection		
Italy	Intrusion Software	Lebanon Army Forces	2015
USA	Off the Air Interception		2011

QATAR

UK	Off the Air Interception		2015
UK	Off the Air Interception		2015
UK	Off the Air Interception		2015
UK	Intrusion Software		2015
Switzerland	Off the Air Interception		2015
Switzerland	Off the Air Interception		2015
Germany	Unknown		2013
USA	Deep Packet Inspection		
Switzerland	Off the Air Interception		2016
Switzerland	Off the Air Interception		2016
Switzerland	Off the Air Interception		2016
Switzerland	Off the Air Interception		2016
Switzerland	Off the Air Interception		2016
Switzerland	Off the Air Interception		2016
Switzerland	Off the Air Interception		2016
UK	Off the Air Interception		2015
UK	Intrusion Software		

MOROCCO

UK	Intrusion Software	Conseil Superieur De La Defense Nationale (CSDN) Unknown other entities	
Finland	Off the Air Interception		2014
Finland	Off the Air Interception		2014
Germany	Unknown		2013
Germany	Unknown		2010
Germany	Unknown		2009
Italy	Intrusion Software	CSDN	2009
Italy	Intrusion Software	Morocco - DST	2012

SAUDI ARABIA

UK	Intrusion Software		
UK	Off the Air Interception		2015
UK	Off the Air Interception		2015
UK	Intrusion Software		2015
Germany	Unknown		2007
USA	Deep Packet Inspection	Saudi Telecom	
USA	Deep Packet Inspection		
Italy	Intrusion Software	GIP Saudi	2010
Italy	Intrusion Software	Saudi - GID	2012
Italy	Intrusion Software	MOD Saudi	2013
Denmark	Unknown		

JORDAN

UK	Intrusion Software		
UK	Intrusion Software		2015
Switzerland	Off the Air Interception		2013
USA	Deep Packet Inspection		
USA	Off the Air Interception		2011
USA	Off the Air Interception		2012
USA	Off the Air Interception		2014

TUNISIA

Denmark	Monitoring Centre, Deep Packet Inspection, Fibre Probes	Government of Tunisia	
Germany	Monitoring Centre	Government of Tunisia	
Germany	Lawful Interception	Government of Tunisia	
UK	Off the Air Interception		2015
Finland	Off the Air Interception		2014
Finland	Off the Air Interception		2014

OMAN

Switzerland	Intrusion Software	Government of Oman	2010
UK	Intrusion Software		
UK	Off the Air Interception		2015
UK	Intrusion Software		2015
Germany	Unknown		2010
Italy	Intrusion Software	Oman - Intelligence	2011
UK	Off the Air Interception		2015
Germany	Lawful Interception		
UK	Lawful Interception		

PALESTINE

USA	Deep Packet Inspection		

SYRIA

Ireland	Network Infrastructure and Services	MTN Syria (mobile operator)	2010
Italy	Monitoring Centre	225, Syrian intelligence	2009
Ireland	Network Infrastructure and Services	Syriatel Mobile Telecom	2008
USA	Network Infrastructure		2011
France	Deep Packet Inspection, Fibre Probes	225, Syrian intelligence	2009
Germany	Monitoring Centre	Syriatel	2009
Germany	Network Infrastructure, Monitoring Centre, Lawful Interception	Syriatel	2000
Germany	Network Infrastructure, Monitoring Centre, Lawful Interception	Syriatel	2007
Germany	Lawful Interception	225, Syrian intelligence	2009
USA	Deep Packet Inspection		
USA	Off the Air Interception		2012

IRAQ

UK	Off the Air Interception		2015
USA	Deep Packet Inspection		
UK	Off the Air Interception		2015
USA	Off the Air Interception		2007

Surveillance technologies & military applications

Surveillance technologies and techniques used for civilian law enforcement are also used in military and counter terrorism applications by armed forces, part of a wider trend to utilize electronic intelligence and autonomous systems over human involvement.

Phone monitoring technology can also be used to identify an individual for a strike. In 2014, a former US drone operator revealed that the CIA and military were using metadata from mobile phones obtained by the NSA for drone strikes and night raids.[112] In the same way that IMSI catchers, described in Annex 1, are used by US law enforcement agencies aboard light aircraft to identify mobile phones, for example after the attacks in San Bernardino,[113] they can also be fitted on drones to identify phones for assassination. The former operator is quoted as saying "We're not going after people – we're going after their phones, in the hopes that the person on the other end of that missile is the bad guy." Infamously, a former director of the NSA and the CIA, General Michael Hayden, has also stated that "We kill people based on metadata."[114] IMSI catchers can also be used to provide tactical intelligence to armed forces engaged in conflict.[115] For example, Israel Aerospace Industries, an arms company and producer of drones, also produces IMIS catchers specifically for mounting upon helicopters and aerostats.[116]

Hacking techniques used in intrusion products are also employed for espionage and sabotage by nation states. The commercial intrusion surveillance technology on the market essentially makes the process of hacking into an individuals phone or computer easier and systematic. Intrusion works by installing malicious code, or malware, onto a device. The malware can then carry out functions unknown to the device's owner and without their permission. For example, it could access data, take a screenshot, switch on the webcam, or switch on the microphone, and subsequently transmit the data elsewhere. In this way such technologies are extremely invasive, by passing any forms of encryption and IT security measures as well as having the ability to modify data. The companies selling commercial intrusion products on the market aim to minimise the burden and expertise involved in this process by offering training and the required software and hardware solutions.

112 https://theintercept.com/2014/02/10/the-nsas-secret-role/

113 http://www.dailymail.co.uk/news/article-3356608/So-terrorists-Homeland-Security-deployed-hi-tech-spy-plane-scoops-tens-thousands-phone-calls-one-time-San-Bernardino-days-massacre.html

114 http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/

115 http://www.defensenews.com/story/defense/land/army/2015/05/13/israel-ground-forces-maneuvering-armor-vehicles-precision-unmanned-robotics-tank/26968519/

116 http://www.iai.co.il/Sip_Storage//FILES/7/36827.pdf

In order to install the malware, targets can be send fake attachments within emails or other communications. It is also possible to install intrusion technologies at a network level within the Internet Service Providerss, meaning that malware can be delivered simply by an individual going on a specific website or updating a specific programme, such as a browser.

Malware can also be delivered using exploits. An exploit is software code which takes advantage of vulnerabilities in code to carry out a specific function. An exploit which takes advantages of wholly unknown vulnerabilities, that is the manufacturer of the product does not know that a vulnerability exists, is known as a zero day exploit. The discovery of zero day exploits can be extremely valuable – companies may pay for information about vulnerabilities in their products, for example. Hackers and governments also buy and use zero days and other exploits for offensive purposes and for surveillance. This has led to a white, black, and grey market for such code. Companies such as French-based VUPEN, now known as Zerodium and based in Washington D.C,[117] sell exploits to government agencies such as the NSA.[118] Surveillance companies selling intrusion also purchase exploits to then re-sell to customers.[119] Hacking Team, for example, paid one exploit developer $45,000 for a single exploit for Adobe Flash.[120] In the same way that this exploit code can be used for surveillance, it can also be used for espionage and sabotage. Stuxnet for example, the attack against Iran's nuclear centrifuges developed by the US and Israel, used four zero days.[121] Edward Snowden claims that in 2012 the NSA inadvertently cut off Syria's entire internet when it attempted to remotely install an exploit within the state ISP to monitor the country's communications.[122]

117 http://www.pcworld.com/article/3000637/security/winner-claimed-in-1-million-ios-9-hacking-contest.html

118 http://www.zdnet.com/article/nsa-purchased-zero-day-exploits-from-french-security-firm-vupen/

119 https://www.privacyinternational.org/node/447

120 http://arstechnica.co.uk/security/2015/07/how-a-russian-hacker-made-45000-selling-a-zero-day-flash-exploit-to-hacking-team/

121 http://www.buzzfeed.com/jamesball/us-hacked-into-irans-critical-civilian-infrastructure-for-ma#.wwrW49AkP

122 http://www.wired.com/2014/08/edward-snowden/

Intelligence collection cooperation

Advanced intelligence agencies appear to be encouraging, developing, and utilizing the surveillance capabilities of foreign states. Reports show there is significant agency to agency cooperation between the countries in the MENA region and Western intelligence agencies. Among the documents provided by Edward Snowden was an internal NSA blog written in 2009 stating that the agency would "share advanced technologies [with third parties] in return for that partner's willingness to do something politically risky."[123] Under RAMPART-A, a programme revealed by Snowden, foreign partners "provide access to cables and host U.S. equipment" in exchange for access to intelligence. The Intercept reports that there have been 13 such data collection points on submarine cables across the world, 9 of which were active in 2013.[124] In a separate file, Algeria, Israel, Jordan, Saudi Arabia, Tunisia, Turkey, and the United Arab Emirates are listed as approved SIGINT partners for the NSA.[125] In 2014, it was reported that GCHQ had a similar programme in Oman, tapping submarine cables.[126]

Access to the submarine cables in strategic points across the world is of high strategic value, given that the vast majority of international internet traffic travels through them, including that of other countries' and not just that of individuals from the country in which the collection point is situated. The role of the private sector in facilitating this collection or providing the necessary surveillance technology is unknown.

123 http://www.duncancampbell.org/content/nsa-inside-five-eyed-vampire-squid-internet

124 https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/

125 http://www.duncancampbell.org/content/nsa-inside-five-eyed-vampire-squid-internet

126 http://www.theregister.co.uk/2014/06/03/revealed_beyond_top_secret_british_intelligence_middleeast_internet_spy_base/

Phone monitoring and analysis technology are used to identify military targets. For example, a June 2012 document leaked by Snowden describes SKYNET, an analysis programme which looks for patterns and behaviours within the metadata of mobile phones.[127] When a mobile phone is connected to a network, it communicates with base stations in the area and sends information to the telecommunications operator for billing and other purposes. The NSA presentation appears to show that the NSA receives this information from the telecommunications providers in Pakistan. Using this metadata, SKYNET sought to identify phones which could indicate whether it belonged to an individual of intelligence value, such as a courier. For example, the metadata could show that the individual was repeatedly visiting locations of interest. It is not known how the NSA accesses this intelligence, whether it is the Pakistani intelligence agencies which initially use phone monitoring technology (Pakistan is an approved third party) and subsequently share it, or whether the NSA obtains it unilaterally, either in cooperation with Pakistani partners by using phone monitoring technology or by hacking.

127 https://theintercept.com/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list/

Regulatory Mechanisms

Given the strategic value of some surveillance technologies and their human rights implications, several regulatory mechanisms by various countries aimed at governing their trade have been initiated, and there have also been calls for industry standards.

Self regulation by the surveillance companies themselves is a crucial mechanism. In 2014, the UK government and Tech UK, an industry association, produced guidelines for companies to assess the risk to human rights posed by exports of cyber security technologies by conducting due diligence and post monitoring practices.[128] In 2011, the Electronic Frontier Foundation, a NGO based in the US, published a "Know Your Customer" guide for surveillance companies.[129]

Some surveillance technologies have been incorporated into sanctions regimes. The EU has embargoed the transfer of surveillance technologies as part of Restrictive Measures against 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." Similar measures were imposed within Council Regulation (EU) No 264/2012 targeting Iran on a broad range of surveillance technologies, as well as technology and software used for their development and use.[130] The items included:

- Deep Packet Inspection equipment
- Network Interception equipment including Interception Management Equipment (IMS) and Data Retention Link Intelligence equipment
- Radio Frequency monitoring equipment
- Network and Satellite jamming equipment
- Remote Infection equipment
- Speaker recognition/processing equipment
- IMSI, MSISDN, IMEI, TMSI interception and monitoring equipment
- Tactical SMS /GSM /GPS /GPRS /UMTS /CDMA /PSTN interception and monitoring equipment
- DHCP/SMTP, GTP information interception and monitoring equipment
- Pattern Recognition and Pattern Profiling equipment
- Remote Forensics equipment
- Semantic Processing Engine equipment
- WEP and WPA code breaking equipment
- Interception equipment for VoIP proprietary and standard protocol

128 https://www.techuk.org/images/CGP_Docs/Assessing_Cyber_Security_Export_Risks_website_FINAL_3.pdf

129 https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment

130 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:087:0026:0036:EN:PDF

It has been suggested that surveillance technologies could potentially be included within the general scope of restricted items within EU and UN sanctions. In February 2014, Privacy International contacted United Nations investigators monitoring the UN arms embargo on Sudan regarding the fact that Hacking Team's technology was reported by Citizen Lab to be in use by the country's military intelligence agency. It was subsequently reported that after the UN Sudan investigators approached the company, Hacking Team replied to say that they had no active business contracts in place. The UN followed up by asking whether there have been any historical contracts. The hack of the company's internal systems showed that in 2012, Sudan's National Intelligence and Security Service paid a total of 960,000 euros for their intrusion system, and that Hacking Team cut off the account's service on November 24, 2014.[131] In response to the UN, Hacking Team stated that its product was not covered by the EU embargo, to which the UN answered that as "such software is ideally suited to support military electronic intelligence (ELINT) operations it may potentially fall under the category of "military... equipment" or "assistance" related to prohibited items.[132] Hacking Team also sold surveillance technology to a military research agency in Russia that works with the FSB, against which the EU had Restrictive Measures.[133] Dutch MEP Marietje Schaake, a leading proponent of stronger safeguards over surveillance technologies within the European Parliament, asked a Parliamentary Written Question to the European Commission regarding the potential violation of sanctions rules, which it instead referred to Italian authorities.[134]

In 2010, the US prohibited the export of "sensitive technology" 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." This provision was later expanded to include Syria through the Iran Threat Reduction and Syria Human Rights Act of 2012, Executive Order 13606 (the GHRAVITY E.O.) and Executive Order 13628.[135] In 2013, a Dubai-based distributor paid a fine of $2.8 million for shipping internet monitoring technology worth $1.4 million produced by Blue Coat to Syria, falsely claiming it was for Iraq and Afghanistan.[136]

131 https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/

132 https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/

133 http://www.forbes.com/sites/thomasbrewster/2015/07/09/wikileaks-hacking-team-fsb-sales/#7819171a5557

134 http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2015-010931&language=EN

135 https://cihr.eu/wp-content/uploads/2014/06/Uncontrolled-Surveillance_March-2014.pdf

136 http://www.reuters.com/article/syria-sanctions-fine-idUSL6N0DC4W120130425

Trade controls

Strategic trade controls imposing export licensing requirements on specific surveillance technologies have also been imposed. The Wassenaar Arrangement has for decades controlled the export of cryptography, meaning that some surveillance systems are subject to prior licensing if they contain certain levels of cryptography.

In 2010, "laser microphones" were added to list, which are used to eavesdrop on conversations by monitoring sound vibrations using lasers, for example through glass.[137]

In 2012, phone monitoring technology was explicitly added to the Wassenaar list to target mobile and satellite phone monitoring equipment. Prior to 2012, some states had already controlled the equipment because of controls on 'Telecommunications systems, equipment, components', though this was interpreted differently by participating states.[138]

In 2013, two further controls were added into the Wassenaar list, one on intrusion software and another on internet monitoring technology.[139] The public statement stated that the controls were aimed at "surveillance and law enforcement/intelligence gathering tools and Internet Protocol (IP) network surveillance systems or equipment, which, under certain conditions, may be detrimental to international and regional security and stability."[140]

The category on internet monitoring, known as IP Network Surveillance Systems, was initiated by France after evidence emerged that a French company, Amesys, supplied internet backbone monitoring technology to Gaddafi's Libya. According to the Wall Street Journal, Amesys' Eagle monitoring centre, which used a combination of probes using Deep Packet Inspection technology and analysis software, was "deployed against dissidents, human-rights campaigners, journalists or everyday enemies of the state" in Libya.[141] A criminal case against Amesys for complicity in acts of torture by the Gaddafi regime is ongoing.[142] France implemented the control almost immediately after it was approved by the WA in 2013.

137 http://www.wassenaar.org/wp-content/uploads/2015/06/Revised-Summary-of-Changes-to-Control-Lists.pdf

138 http://www.cecimo.eu/site/fileadmin/documents/EU%20LEGISLATION%20AND%20DOSSIERS/Dual-use_legislation/FINAL_REPORT.pdf

139 https://cda.io/r/ConsiderationsonWassenaarArrangementProposalsforSurveillanceTechnologies.pdf

140 http://www.wassenaar.org/wp-content/uploads/2015/06/WA-Plenary-Public-Statement-2013.pdf

141 http://online.wsj.com/news/articles/SB10001424052970203764804577056230832805896.

142 http://businesshumanrights.org/en/amesys-lawsuit-re-libya-0#c18496.

The addition of items related to intrusion software were proposed by the United Kingdom and also agreed at the WA in December 2013. The UK government has stated that these controls were on "Complex surveillance tools which enable unauthorised access to computer systems"[143] introduced "because of real concerns about the use of such tools to breach human rights and the risks that they pose to national security".[144] The controls distinguished between components used to create and control the malware itself, meaning that the malware component is not targeted, but rather the command and control infrastructure used to generate, install and instruct the malware.[145]

The 2013 additions to the Wassenaar list were added into the EU Dual Use regulation in January 2015. The regulation, which is binding on member states, incorporates decisions to include items for licensing restrictions taken at Wassenaar level, meaning that member states have been controlling the 2013 items since then.

In July 2015, the US Bureau of Industry and Security (BIS) published a proposed implementation of the 2013 additions, causing widespread concern among IT security researchers relating specifically to the implementation of controls on intrusion software. Concerns largely revolved around the fact that the US had interpreted the international agreement too broadly and that the language used by BIS could be interpreted to cover the development of malware and sharing of information about vulnerabilities, meaning that researchers would have would have to apply for an export license before sharing information about vulnerabilities. Since an open round of submissions, BIS has since agreed to reinterpret the agreement and attempt to update the control language within the Wassenaar Arrangement itself.

Israel is not a participating member of the Wassenaar Arrangement, although it does include items added to the Wassenaar Arrangement's control list within its own list of strategically controlled goods. In January 2016, the Israeli Defense Exports Control Agency published proposed rules aiming to make a broad range of technologies that can be used for surveillance subject to licensing, going further than any other participating country and far beyond what was decided at the Wassenaar Arrangement, by explicitly stating that the export of exploits would be regulated.[146] Amid significant opposition from Israeli defence contractors,[147] in April it was reported that the Israeli authorities scaled back many of the proposals.[148]

143 https://www.techuk.org/images/CGP_Docs/Assessing_Cyber_Security_Export_Risks_website_FINAL_3.pdf

144 http://blogs.bis.gov.uk/exportcontrol/files/2015/08/Intrusion-Software-Tools-and-Export-Control1.pdf

145 https://cda.io/r/ConsiderationsonWassenaarArrangementProposalsforSurveillanceTechnologies.pdf

146 http://www.gkh-law.com/cyber-update-february-2016/

147 http://www.defensenews.com/story/defense/policy-budget/cyber/2016/01/26/israeli-govt-reaches-out-before-clamping-down-cyber-exports/79364842/

148 http://www.globes.co.il/en/article.aspx?did=1001119266&from=iglobes

Since 2011, and around events during the Arab Uprising, the EU has been conducting a review of the Dual Use Regulation. In 2011, the European Commission published a Green Paper and call for evidence, followed by a report on the public consultation being adopted in January 2013. Regarding surveillance technology, the Commission Communication published in 2014 recognised the risk posed by "the emergence of specific 'cybertools' for mass surveillance, monitoring, tracking and interception", while importantly also recognising "the interlinkages between human rights, peace and security".[149] Privacy International through the Coalition Against Unlawful Surveillance Exports (CAUSE)[150] is campaigning for the regulation to mandate that member states require companies to apply for an export license for all types of surveillance technologies where practically possible, that they appropriately assess human rights risks in the assessment process, and that report data about granted and denied licenses to foster transparency and accountability.

Any changes to the Regulation will need to be agreed upon by all member states, as well as by the European Parliament. The Parliamentary Subcommittee on Human Rights and the Committee on International Trade convened a hearing on surveillance technologies in January 2015. In April 2015, the Foreign Affairs Committee of the European Parliament adopted a report by MEP Marietje Schaake on Human rights and technologies: the impact of digital surveillance and intrusion systems on human rights in third countries, which was approved by the parliament in Autumn 2015.[151]

The Commission also initiated an impact assessment aimed at informing the policy-making process by quantifying and providing objective data on the industry and the potential cost of any regulatory changes. Ecorys, a European research and consultancy company, in partnership with SIPRI, carried out a data collection project, including a component specifically focused on surveillance technologies, to inform the impact assessment. The report was submitted to the Commission in November 2015 and provides a broad and detailed analysis of the European market for surveillance technologies and policy issues.[152] The Commission also initiated an online consultation on potential regulatory changes.[153]

Simultaneously, a Subcommittee, the Surveillance Technology Working Group (STEG), was established within the DG Trade Dual Use Working Group. Consisting of experts from the national licensing authorities in Germany, the Netherlands, Finland, Sweden, Denmark, the UK, France and Poland, the working group is aimed at identifying surveillance technology that poses a risk to human rights and how it can be effectively controlled.

The European Commission is due to publish a draft proposal in late 2016.

149 http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2014_trade_014_dual_use_en.pdf

150 CAUSE is a a coalition of NGOs consisting of Access, Amnesty International, Digitale Gesellschaft, Human Rights Watch, the International Federation for Human Rights (FIDH), the Open Technology Institute at the New America Foundation, and Reporters Without Borders.

151 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2015-0178+0+DOC+XML+V0//EN

152 http://www.sipri.org/news/EU-dual-use-review

153 http://trade.ec.europa.eu/consultations/index.cfm?consul_id=190

In August 2015, Germany unilaterally announced a Federal amendment to its laws seeking "to stop the use of [surveillance] technology for internal repression in countries of destination." Germany also added new surveillance items to its list of technologies which require export authorisation, covering monitoring centres and lawful interception technologies. In announcing the new regulations, the Vice Chancellor of Germany, Sigmar Gabriel, stated that "human rights violations can not only [occur] with weapons, but ultimately with technologies for example, wiretapping. So far the European regulations for the export of such technologies to other countries is sketchy. The Federal Government is therefore closing the gaps, [which are] still under discussion in Brussels. We will work in Brussels, as well as internationally, for speedy European and global regulations."[154]

Switzerland has also taken unilateral steps. After an investigation by Privacy International in conjunction with Swiss magazine WOZ, it was uncovered that representatives from a Bangladeshi unit dubbed a "death squad" by Human Rights Watch were being hosted in Zurich by a manufacturer of IMSI Catchers, NeoSoft.[155] By 2011, over 700 extrajudicial executions had been carried out by the RAB over seven years since its formation in 2004, according to Amnesty International.[156] Because such training would require an export license, and authorities confirmed that none was sought, the company was referred to federal prosecutors for a potential violation of export control laws.[157] Additional Director General of RAB, Colonel Ziaul Ahsah, subsequently reported to Bangladeshi media that the export had been stopped "just before the shipment of the materials" by Switzerland after "a human rights organisation reported against RAB."[158]

In May 2015, the Swiss Federal Council added an amendment to their export regulations which for the first time compels the export control authorities to deny all license applications for internet and phone monitoring technology if there is "a reason to believe" that the export may be used "as a means of repression".[159]

As of February 2016, the data now shows that 95 separate permanent and temporary licenses for IMSI Catchers have been granted by the Swiss government since 2012. Since the new law has been in place, two applications for IMSI catchers have been denied, to Vietnam and Bangladesh.[160] No applications have been received for any other surveillance technology since then, even though Switzerland was home to a large number of surveillance companies. In July 2015, it was reported in Swiss media that some surveillance companies have vacated their offices and left Switzerland as a result of the new law.[161]

154 http://www.bmwi.de/DE/Presse/pressemitteilungen,did=719188.html

155 https://www.woz.ch/-53af & http://www.rts.ch/info/suisse/6120656-une-entreprise-suisse-de-cybersurveillance-en-affaires-avec-le-bangladesh.html

156 https://www.amnesty.org/en/press-releases/2011/08/bangladesh-government-must-act-now-stop-police-unlawful-killings/

157 http://www.tagblatt.ch/nachrichten/schweiz/tb-in/Heikles-Geschaeft-mit-Big-Brother;art120101,3950361

158 http://www.newsbangladesh.com/english/Switzerland%20holds%20back%20shipping%20of%20intelligence%20gears%20for%20RAB/482.

159 http://www.seco.admin.ch/aktuell/00277/01164/01980/index.html?lang=de&msg-id=57261

160 http://www.tagblatt.ch/nachrichten/schweiz/tb-in/Bern-schraenkt-heikle-Exporte-ein;art120101,4291111

161 http://www.schweizamsonntag.ch/ressort/politik/bund_verscheucht_hersteller_von_spionagesoftware_aus_der_schweiz/

Conclusion

Surveillance technologies are not new. Wiretapping equipment and other electronic technologies used to identify, track, and monitor individuals have been used widely throughout the 20th century. State espionage and civilian monitoring was a common feature throughout the Cold War, in both blocs. The spread of the internet and new communications methods has however both increased the levels of intrusiveness of surveillance, as well as its power. The ability to monitor entire groups and nations on a mass scale poses new and substantially more grave human rights issues. Reforms of surveillance laws undertaken as a direct result of Edward Snowden's disclosures show how even within political systems with significant checks and balances, surveillance capabilities have outstripped the ability of laws to effectively regulate them.[162] In non-democratic and authoritarian systems, the power of surveillance technologies means that they can be used for human rights abuses and undermine democratic development and privacy, a human right essential in allowing individuals control, dignity, and the realisation of other human rights. Individuals have had their communications read to them during torture,[163] while opposition activists have had their entire communications infiltrated and monitored.[164] Intelligence agencies are utilizing modern communications to carry out military attacks, and it's now technically possible for entire opposition movements and large sections of society to be surveilled, systematically and relatively cheaply.[165] [166]

Understanding the role that the private surveillance sector plays in surveillance worldwide is crucial to developing comprehensive safeguards and effective policy. A lack of reliable data makes this difficult however. How the industry functions, the capabilities of the technology, where it is sold, and how it is used, is shrouded in secrecy. Privacy International has collected data within the SII, while what is known about where technologies are sold is only known because of investigative reporting and government transparency because of export licensing restrictions. From the data that is available, it appears clear that surveillance technologies are generally produced and traded from economically advanced large arms exporting states in the northern hemisphere. Exports to countries in the global south and authoritarian countries overwhelmingly come from these states.

162 https://www.theguardian.com/technology/2015/jun/06/surveillance-privacy-snowden-usa-freedom-act-congress

163 http://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking

164 http://apnews.excite.com/article/20150807/lt--ecuador-hacking_the_opposition-18a465a3dd.html

165 https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/

166 https://www.privacyinternational.org/node/816

The fact that the vast majority of surveillance companies and reported sales of technologies come from companies in advanced economies also presents opportunities in terms of regulatory mechanisms. Both sanctions and export licensing restrictions have been used to block specific transfers of surveillance technologies and provide data on their trade. Various states and the EU have pursued instruments to ensure that human rights are appropriately considered within the trade in surveillance technologies. The mechanisms used for this, sanctions and export controls, are mechanisms rooted in the Cold War however, and pose significant difficulties and potential for unintended consequences.

Nevertheless, from what is known about their use and trade, it is clear that safeguards are a matter of urgency. A comprehensive approach should be pursued incorporating export restrictions where possible as well as improved standards in corporate social responsibility.[167] While pro-active due diligence on the behalf of companies is a necessary start, without instruments capable of restricting transfers and shining a light on the companies and the trade, surveillance technologies developed in and traded from the West will further undermine privacy and facilitate other abuses. This will not only undermine the human rights of individuals in some of the most authoritarian countries across the world in the name of security, it will also undermine democratisation itself, leading to instability and, ultimately, international insecurity.

167 Bromely et al, ICT Surveillance Systems: Trade Policy and the Application of Human Security Concerns, StrategicTrade Review, Spring 2016, <http://www.str.ulg.ac.be/wp-content/uploads/2016/03/Strategic-Trade-Review-Issue-02.pdf>

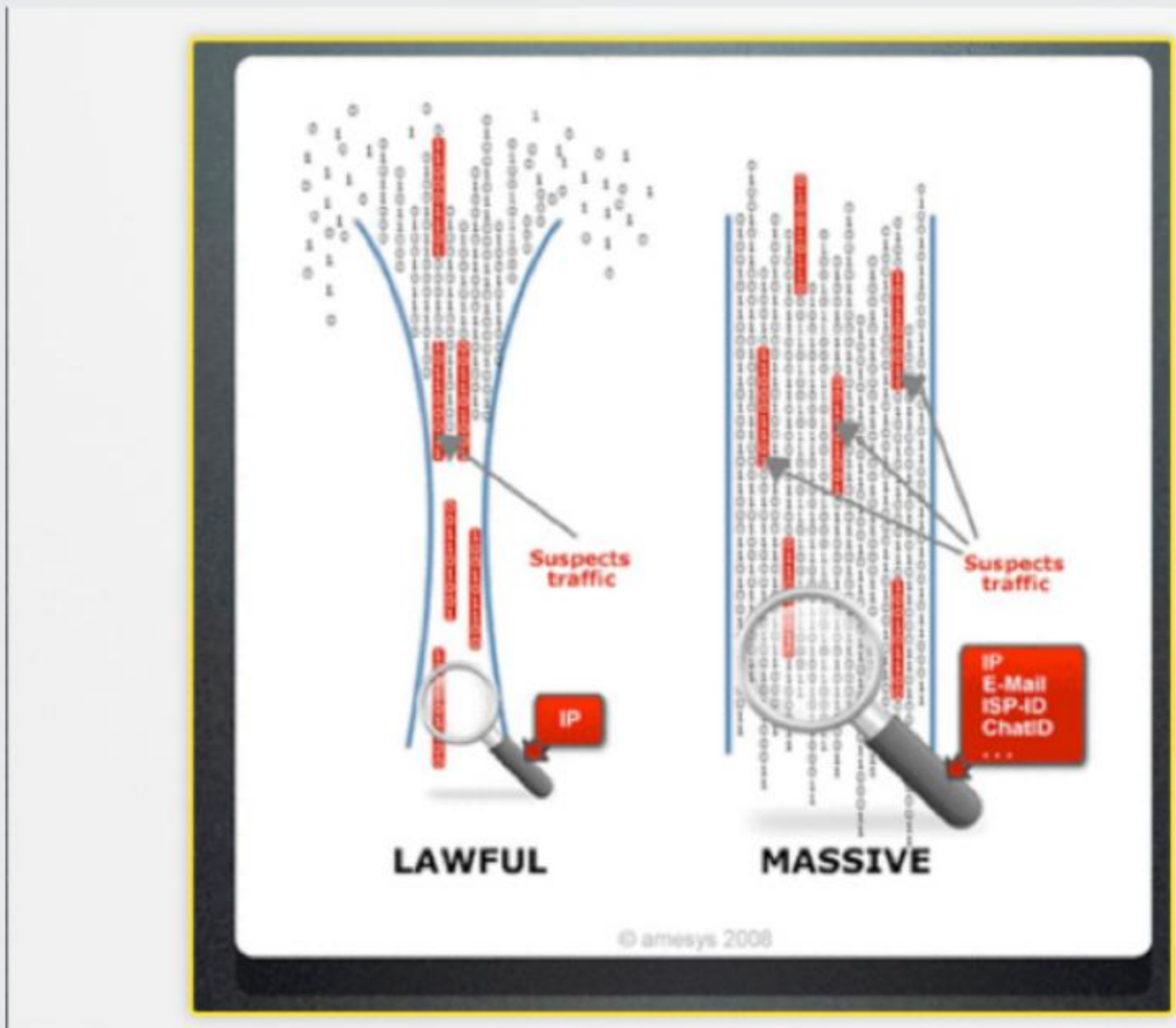
Annex

Surveillance Technology Explainers

The SII as of April 2016 contains 1534 individual brochures of surveillance technologies. There are split into 11 categories. Individual products may fall into more than one category. The diagrams are taken from actual brochures with descriptive text available on the Privacy International website.

Types of Surveillance Technologies

Technology	Description
Internet Monitoring (Includes Deep Packet Inspection & Fibre Taps / Probes)	Technologies that focus on gathering information communicated across the internet



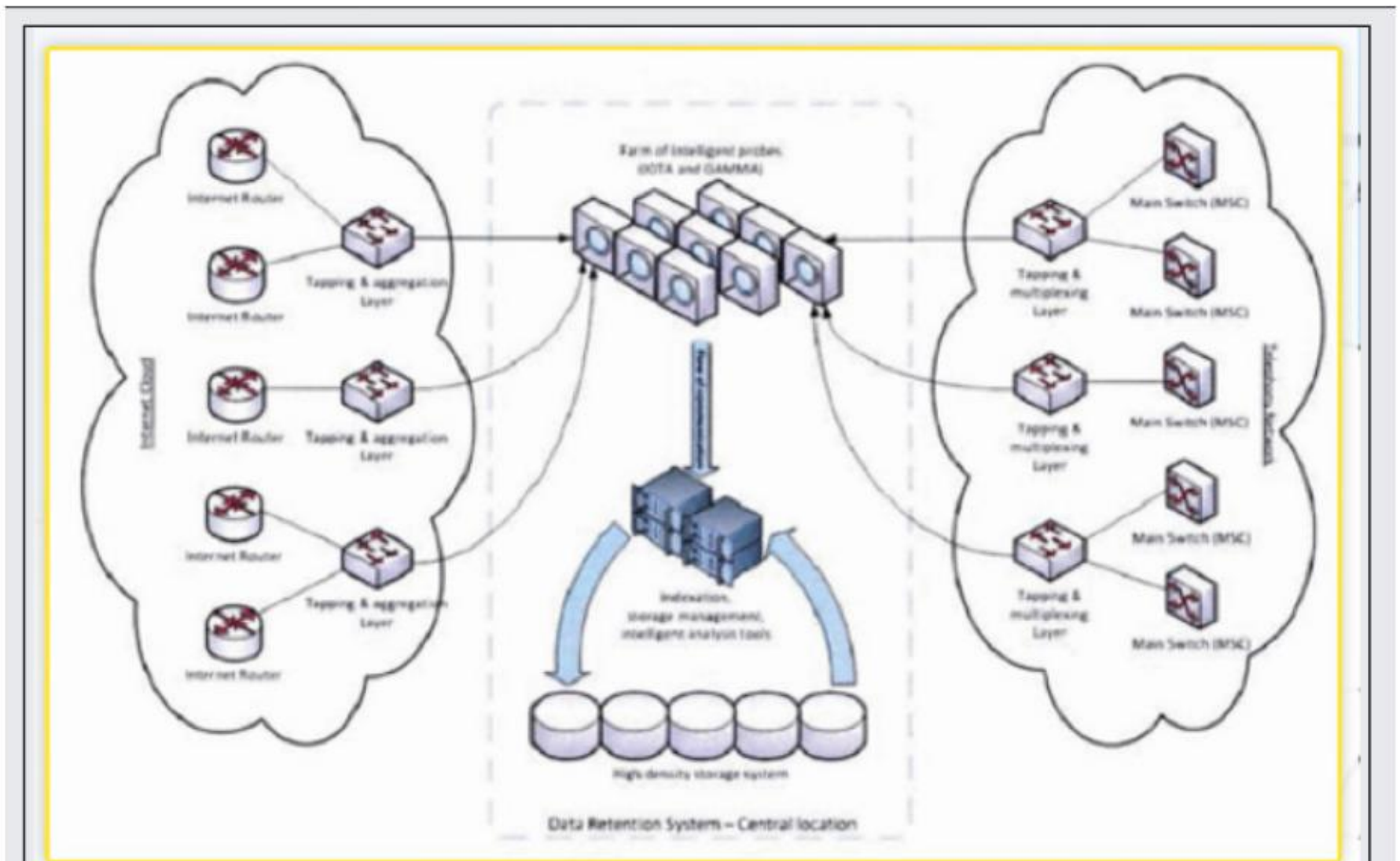
Amesys' Eagle system makes the particular distinction between the two focuses of it's system. The first is Lawful Interception which presumes a legally based framework in which to conduct surveillance, targeting specific suspects and avoiding interception of other content. The other option is Massive, looking at everyone's information as it moves through the communication framework and picking out the information relevant to you. It also implies that there is no legal framework for this type of surveillance either considering the former option. When Amesys provided the

LIMS Access Points for IP services	Cost-effective probes for single IP services like e-mail, VoIP, AAA, SMS, MMS
LIMS Access Points DPI	Deep Packet Inspection Probes for 1Gb to 10Gb Ethernet networks
LIMS Access Points TDM	Probes for circuit-switched networks based on E1/T1, SDH/SONET (STM-1 to STM-4)

LIMS Access Points are the interception probes that Utimaco provides in its Lawful Interception Management System. The three probes focus on interception over IP (Internet Protocols), DPI (Deep Packet Inspection) and TDM (Time Delay Multiplexing).TDM probes are focused on the interception of information coming over a phone network, DPI probes focus on the interception of Computer networks and IP probes focus on electronic communications that can cover both computer and phone networks.

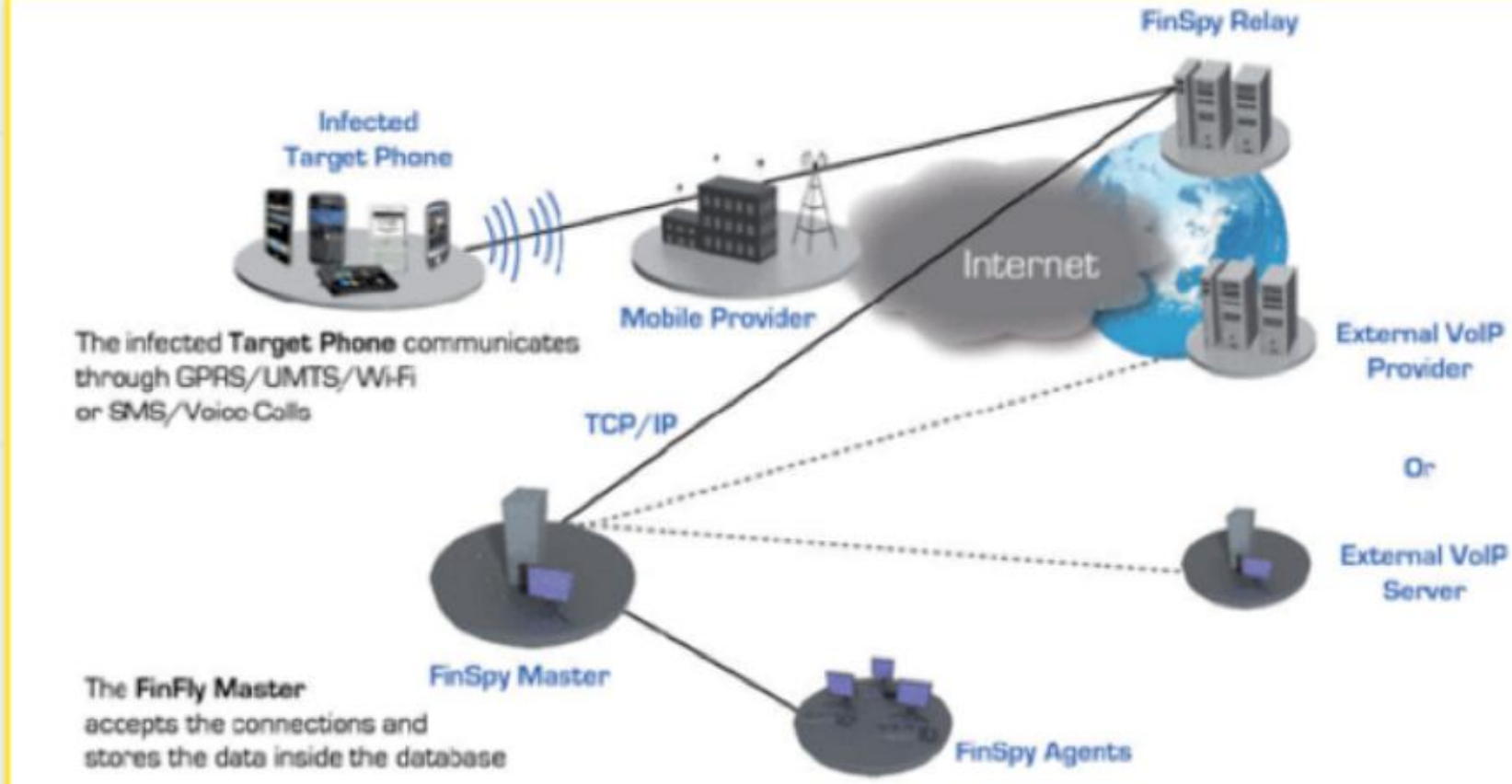
Phone Monitoring (Includes Off the air interception & Lawful Interception technologies)	Technologies that focus on gathering information communicated across mobile, fixed or next generation networks (2G, 3G, 4G)

Neosoft's GSM Monitoring Fully Passive System places itself between the mobile handset and the GSM Provider. It tunes into the signals that are being transmitted between the two points and then begins to decrypt the message or call that is being hosted by the Base Transceiver Station from the handset.



Advanced Middle East Systems' Cerebro Data Retention System provides storage capacity to the Cerebro monitoring centre. Without the DRS the capacity to intercept and analyse, and retain for long periods of time would be seriously constrained. With the system as the company puts "there is no limit to the scalability of the system in terms of storage duration".

Intrusion	Technologies which facilitate the installation of malware onto a person's communication device (mobile or computer), removing information from the device, and taking control of functions such as the webcam and microphone



FinSpy Mobile is Gamma's Mobile Phone edition in the FinFisher product suite. This targets an individuals smartphone by delivering FinSpy onto the target's phone through a fake update (in one particular example). After that point the target's privacy is utterly compromised, his phone is now accessible by FinSpy which harvests contacts, e-mails, Calendar entries, Pictures. It can also surveil the target by making silent calls and using the phone to listen to conversations. Once FinSpy Mobile has been installed on a phone, it can be remotely controlled and monitored no matter where in the world the Target is located.

Monitoring Centre Technologies that combine the focus of Internet Monitoring, Phone Monitoring, even Audio and Video Surveillance, into one suite of technology

Key Benefits

The Nice Track Horizon Insight platform is designed to extract and produce valuable intelligence from vast amounts of intercepted communication data using built-in intelligence know-how and workflows, and innovative algorithmic and analytic data mining capabilities.

Zero-Lead Investigations:

Grants access to all stored data and metadata that may become relevant for monitored targets and new suspects

Built-in Intelligence Know-How:

Provides capabilities to track suspicious and criminal activities based on similar predefined characteristics and communication patterns accumulated over years of experience

Preventive Intelligence:

Detects and alerts suspicious or dangerous activities based on communications patterns to prevent potential criminal acts in real-time

Data Enrichment:

Enables fusion of target and suspect data from various registries and open sources for enriched data

Technology Highlights

Nationwide Collection of High Volume / High Rates Data

Intercepts, formats and stores billions of telephony and IP events per day at a rate of thousands of data records per second

Processing and Normalization Engine

Aggregates, correlates and canonizes data from numerous sources resulting in maximum intelligence credibility

Complex Communication Pattern Alerting Engine

Automatically identifies "under-the-radar" activity, invisible to analysts, using the market-leading *NICE Actimize* pattern analysis technology

Efficient Data Storage and Retrieval

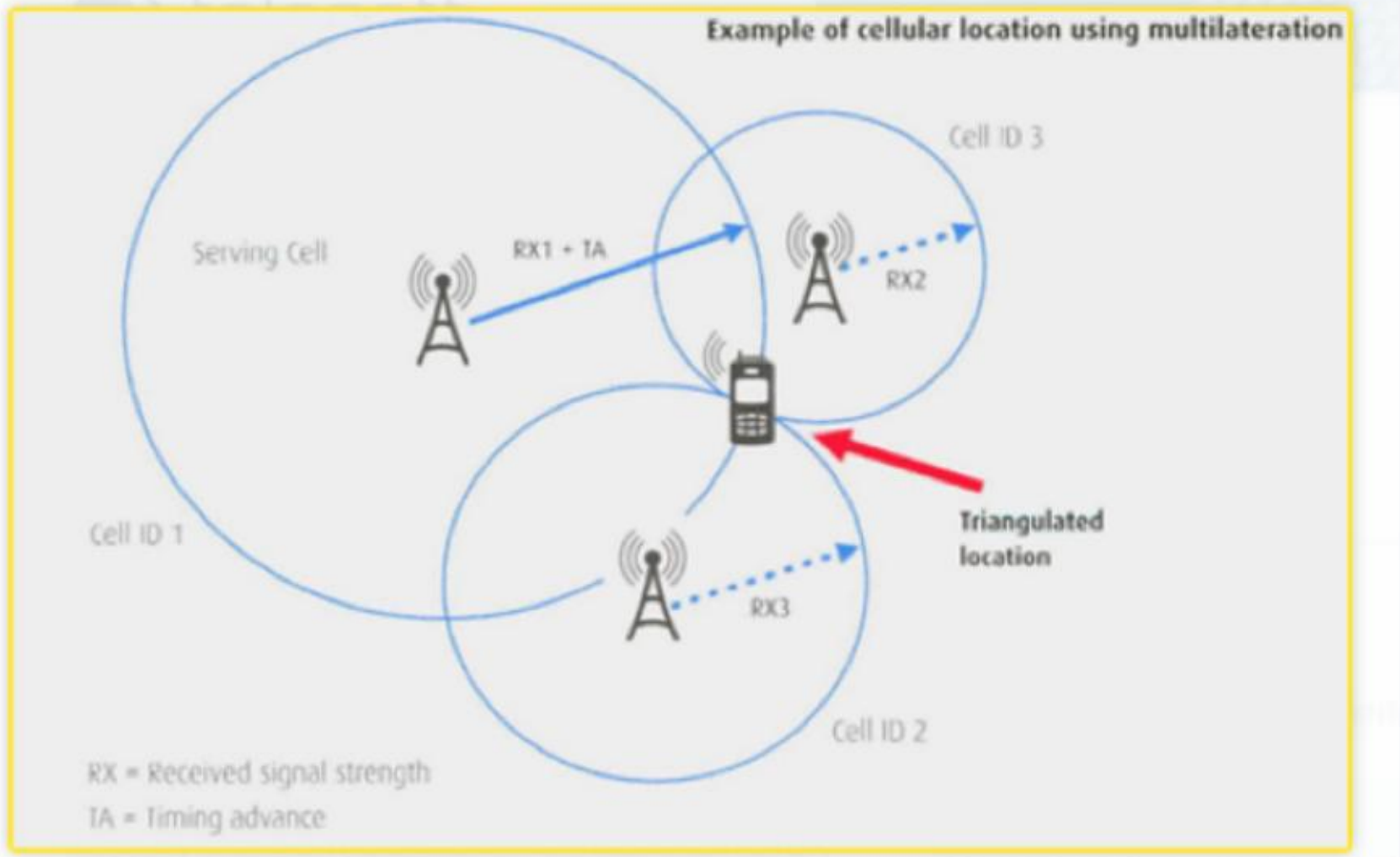
Enables efficient storage for several years, while maintaining quick data retrieval, visualization and analysis

Integration of All Data Sources

Integrates all legacy sources with newly acquired sources in telephony, IP and open source fields to perform fusion of all intercepted data

Nice System's Horizon Insight combines both the tapping of IP and telephony traffic and the analysis of that with open sources to create a massive, sophisticated system that is able to monitor users activity and construct patterns across the intercepted information.

Location Monitoring	Technologies that monitor the location of a target, sometimes using their mobile phone, others using GPS tracking devices placed on the person or their vehicle



The Hinton Abis probe is a mobile location tracking device. It finds the physical location of the mobile phone by watching its signal links between different mobile base stations. Using the Abis signal- hence the name of the probe- provides the GSM (Global System for Mobile Communications) to figure out the distance of the mobile phone from ideally three mobile base stations which it will be sending signals to. This can be used for location-based advertising like Telesoft says, but at its core this is about turning your own mobile phone- one of the most omnipresent pieces of technology on the planet- into a location tracking system.

Biometrics	Technologies that identify and categorise people based on individual characteristics. (Speech Recognition, Facial Recognition, Speaker Identification, Biometrics Database)

FACIAL RECOGNITION (p. 3)

1

Face Image Acquisition

Image acquisition can be done from live or file sources (e.g. from a camera or a .JPG file), still or video images.

During face acquisition, a unique identifier of the acquired image must be allocated .

2

Pre-processing and Image Enhancement

This step aims at finding where the face (or faces) is located in the image, and pinpointing the eye centres.

3

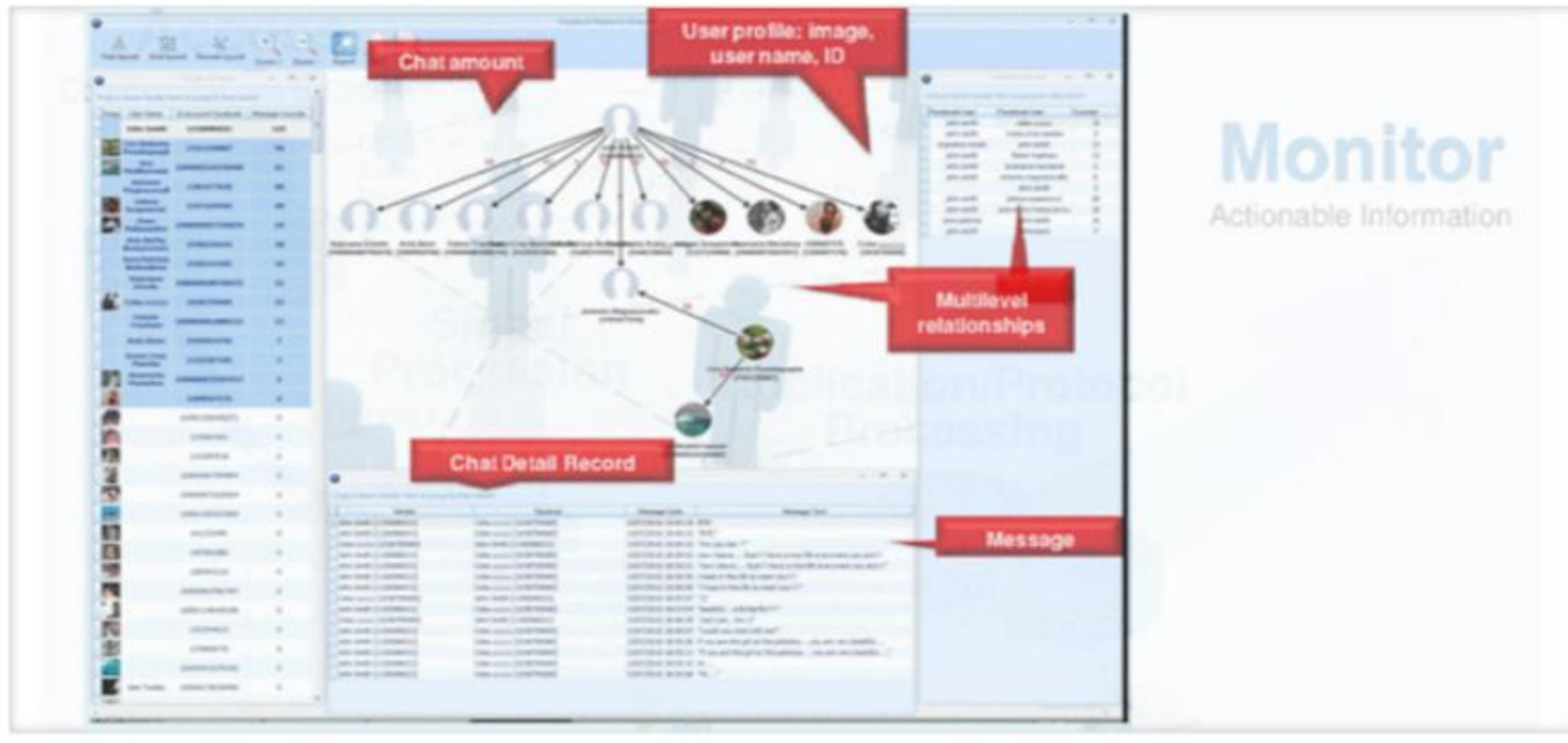
Template Extraction

A template is a representation of the image that is suitable for image comparison. A template may represent either visible features of a portrait (e.g. nose or eyebrows location), or purely mathematical data such as the results of applying one or more filters to all or part of the image.

MorphoFace details how their facial recognition technology works: your image is acquired, processed and then digitised in the form of a template. These steps are all automated by a computer and require little human interaction. Morpho advertises that their technology "can be deployed and used with minimal effort even for users with no or very limited knowledge of face recognition". This ease of implementation regardless of an understanding of the technology and its limitations is disconcerting; the limitations of the technology should always frame how it is used.

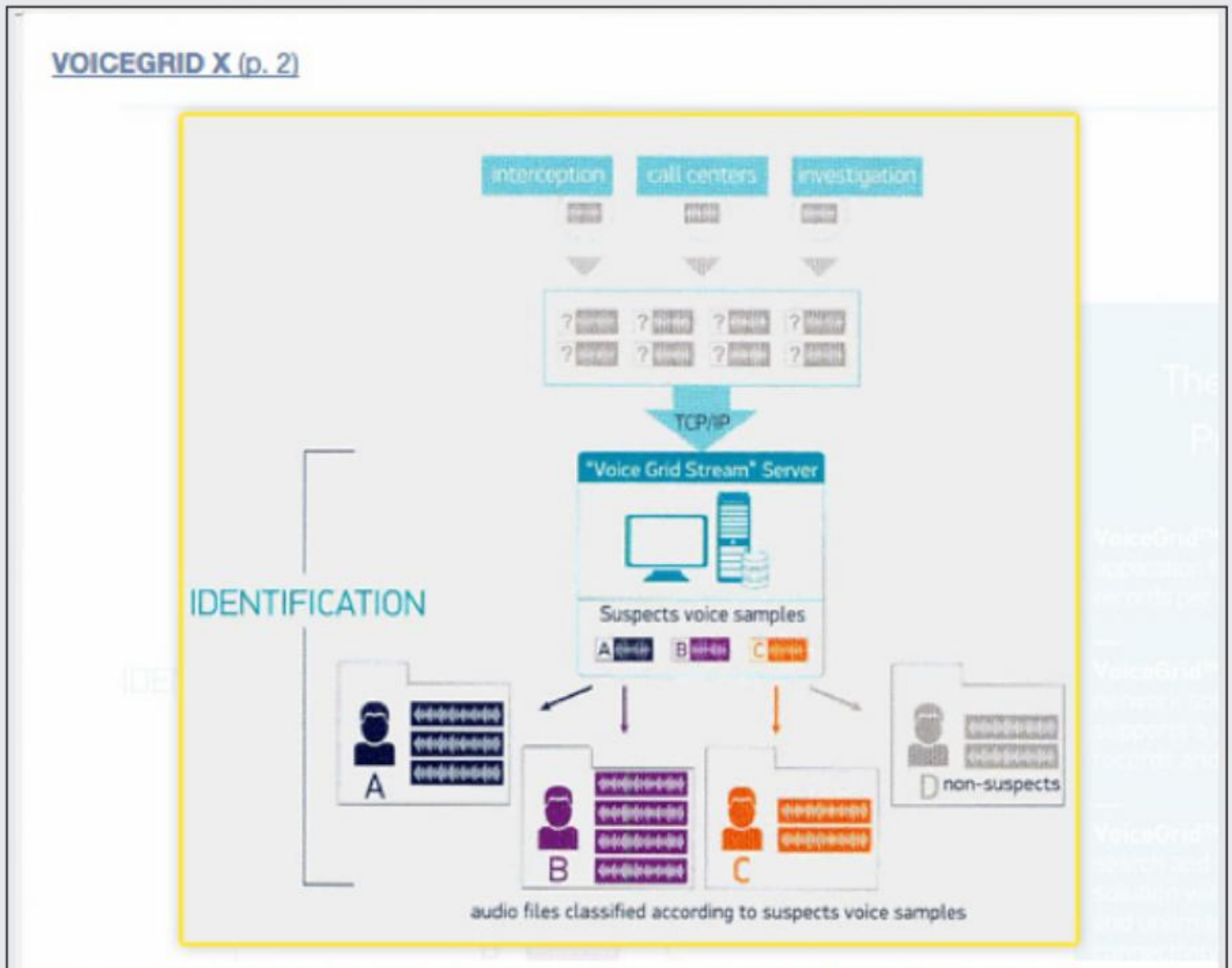
Analysis Technology that uses information gathered from sources such as social networks to map out relationships between monitored users, recognise patterns within data, analyse the meaning of words, etc.

Relationship Mapping over Facebook accounts ◀ PREVIOUS NEXT ▶



Who do you know? Who do you speak to most often? What do you say to your friends? What do they say about you? Glimmerglass advertises the capability to intercept online traffic and analyse Facebook accounts, uncovering huge amounts of personal information about individuals and the people they know. This is a screenshot from IPS' 'Facebook Relations Analysis' software platform.

Audio Surveillance Technologies that surveil by using Audio-based technologies



Speech Technology Center's VoiceGrid X is a part of the VoiceGrid product line designed for speaker identification and surveillance. VoiceGrid X is designed for identification of speakers to a list of targets. The programme can process 10,000 recordings against 100 suspects voice samples. A wide net that is available to be cast.

Video Surveillance Technologies that surveil by using Video-based technologies

UK-based Sonic Communications' line of concealed cameras can be hidden in child safety seats, jackets, tissue boxes, ties, hangers and even in bricks. Sonic Communications also offers a "customised installation service into garments or other 'hosts' supplied by the customer".

Equipment A miscellaneous category, for those things that don't necessarily provide surveillance capabilities but can aid them (vans, computer monitors, UAVs)

The growth in the use of Unmanned Aerial Vehicles for surveillance purposes is alarming. More commonly associated with use in the military arena, Law Enforcement in both Britain and the United States have been turning to Unmanned Aerial Vehicles to monitor large public gatherings or borders.

Counter-Surveillance Technology that detects and counters surveillance

In an age where the threat of surveillance is patently apparent those who can invest in counter-surveillance equipment do. And those who can profit from it are more than happy to do so. QCC's Searchlight is a counter-surveillance tool against GSM surveillance, traditionally deployed to intercept mobile communications.