Mapping the supply of surveillance technologies to Africa

Supply-side report

Sebastian Klovig Skelton and Anand Sheombar

DOI: 10.19088/IDS.2023.027

1. Introduction

The goal of this supply-side report is to map which companies from which countries are exporting surveillance technologies to African governments. The report does not set out to be comprehensive due to finite resources and the limitations of desk-based research into companies that are strategically secretive about their operations. The authors have paid particular attention to exports of surveillance technologies to the five countries featured in the accompanying country reports: Nigeria, Ghana, Morocco, Malawi, and Zambia. Exports to other African countries are mentioned where they help to illustrate wider patterns.

Despite the limitations of the research, our literature review suggests that this report is the most complete mapping to date of surveillance technology exports to the five target countries. Further research is needed to deepen analysis of exports to these five countries and to expand the mapping to other countries on the continent.

This report reviews prior research to provide an overview of what is already known, and it highlights research gaps and opportunities. By collating this information in one place, it is hoped that other researchers will be able to use it as a basis for further, more in-depth investigations.

Our initial review of published accounts of surveillance technology supply contracts revealed that the majority came from the world's largest arms exporters, that is, the countries with the most advanced military and digital technology sectors (Wezeman, Kuimova and Wezeman 2021). The USA, Russia, France, China, and Germany together accounted for 77 per cent of all arms exports between 2017 and 2021. The next largest arms-exporting governments were Italy, the UK, South Korea, Spain, and Israel.

Given the number of European Union (EU) countries in the top ten arms exporters, this report analyses their exports to African governments as a bloc, while highlighting some examples from each as a member state.

Otherwise, the only large arms-exporting country not properly investigated by this report is South Korea, due to time constraints. Israel was included because of the high-profile news stories and extensive research availability following the exposé of Israeli company NSO Group's supply of Pegasus mobile spyware that was employed in several of the focal countries in Africa.

To inform the content of this report, researchers used a variety of open-source databases, including news cuttings, open data on export licences published by governments, academic research into the spread of surveillance equipment, and information openly published by digital surveillance companies, such as press releases and brochures.

2. China

China is a major and growing supplier of digital surveillance technologies to Africa, particularly through the transfer of smart city and telecommunications infrastructure. Although precise figures are hard to verify, China competes head-to-head with the USA to dominate the multibillion-dollar global market for surveillance technologies that use artificial intelligence (AI) (Feldstein 2019). These technologies use AI to conduct keyword searches on big data sets created by intercepting the internet communications and mobile phone calls of all citizens. These technologies are often made available to African governments as part of multimillion-dollar soft-loan-assisted packages that include closed-circuit television cameras (CCTV) that have facial recognition and car number plate recognition capabilities. These surveillance packages, branded variously as 'Safe City' by the Chinese company Huawei, or as 'Smart City' by rival Chinese company ZTE, transmit these multiple streams of surveillance data to a central command and control 'data centre' where citizens can be monitored and tracked in public spaces and online. This mass surveillance system represents a substantive threat to citizens' constitutional rights to privacy, and freedom of association and expression (Gagliardone 2020; Woodhams 2020). These surveillance systems are already operational in whole or in part in Ghana, Zambia, and Malawi (see country reports elsewhere in this publication).

According to Steven Feldstein, technologies linked to Chinese companies are found in at least 63 countries worldwide, and Huawei alone is responsible for providing AI surveillance technology to at least 50 countries (Feldstein 2019: 2). He noted: 'Chinese product pitches are often accompanied by soft loans to encourage governments to purchase their equipment.'

The primary vector for the transfer of digital surveillance technology from Chinese firms to African governments is the 'Digital Silk Road' (DSR), which is the part of China's 'Belt and Road Initiative' (BRI) that focuses on improving information and communications technology infrastructure capabilities in other states. The DSR cuts across multiple areas of technology, including 5G, data centres, e-commerce, smart cities, smartphones, undersea fibre-optic cables, the 'internet of things' (IoT), AI, and financial technology (fintech). According to the Green Finance Development Centre, 147 countries globally had joined the BRI as of March 2022 after signing a memorandum of understanding (MoU) with China, including 43 countries from sub-Saharan Africa and 18 from the Middle East and North Africa (Nedopil 2023). This includes all the countries in the scope of this report.

China’s involvement in Africa also predates the BRI and can be traced back to the government’s ‘go out policy’, which was launched in 1999 with the aim of promoting the internationalisation of Chinese companies. Participation in the BRI does not automatically mean a country is also involved in the DSR, although it does mean there is potential for them to be.

The supply of large digital systems from China is often enabled by soft loans from China. According to the Chinese Loans to Africa (CLA) database – an interactive data project developed by Boston University Global Development Policy Center that tracks loan commitments from Chinese entities to African governments and state-owned enterprises – there have been a total of 1,188 loans amounting to US$159.9bn since 2000 (Boston University Global Development Policy Center 2022). It is impossible to tell which are specifically DSR-related.

The CLA database shows that, of the total, 148 loans collectively worth US$13.5bn were related to information and communication technologies. The database only contains information from publicly available sources. Many of these loans are for IT infrastructure projects, rather than direct surveillance capabilities, although many of the technologies being transferred could potentially be repurposed for surveillance. There are also no IT loans to Morocco mentioned in the database.

Significant loans include:

- **Ghana:** US$150m and US$199m respectively for Phase I and Phase II of the Integrated National Security Communications Enhancement Network (ALPHA) Project, a nationwide safe city project in Ghana. The Ghanian government signed an MoU with China’s Ministry of National Security, Huawei, and China Machinery Engineering Corporation (CMEC) (Ofori-Atta and Kan-Dapaah 2019). In November 2013, Ghana received a US$129m loan from the Export–Import Bank of China (China Exim Bank) for the extension of dedicated security information infrastructure, including an ‘intelligent video surveillance’ component, implemented by Huawei and ZTE (AidData n.d.).
- **Nigeria:** US$200m for a Nigerian Communications Satellite (NIGCOMSAT) in 2006; a ‘replacement project’ for the satellite worth US$20m in 2010; a Public Security Communication System Project worth US$400m in 2010; and two phases of a National ICT Infrastructure Backbone project in 2013 and again in 2018, respectively worth US$100m and US$334m (Abdulaziz 2023).
- **Zambia:** Eight different IT-related loans worth US$958m, including for fibre-optic cables, a public security network, communication towers,

and a Smart Zambia National ICT Development Project. Huawei (2022) noted on its website that it is 'the primary project supplier'.

- **Malawi:** There is one IT loan for a National Fibre Backbone in 2016 worth US$23m.

These loans come from a variety of sources within China, including 'policy banks' (which are the biggest lenders at US$125bn) and commercial banks (such as the Industrial and Commercial Bank of China (ICBC), China Exim Bank, and China Minsheng Bank), various Chinese government entities, the China International Development Cooperation Agency (CIDCA), and individual 'contractors' such as Huawei and ZTE.

- Huawei is active in Ghana, Nigeria, Zambia, Malawi, and Morocco, and is most associated with the deployment of safe/smart city technologies (Huawei 2020, 2021, 2022; Burkitt-Gray 2022).
- In 2015, Huawei launched a US$1.5bn fund to support the development of smart cities across Africa (Takouleu 2018), which has been used to support projects in Ghana (such as ALPHA), Nigeria, Rwanda, South Africa, and Kenya, and has been extensively involved in setting up digital infrastructure in Zambia (*China Daily* 2022), where *The Wall Street Journal* reported it helped authorities intercept encrypted communications and use mobile data to track political opponents (Parkinson, Bariyo and Chin 2019a). Huawei emphatically denied the allegations (Parkinson, Bariyo and Chin 2019b).
- ZTE, on the other hand, has subsidiaries in Ghana, Nigeria, and Zambia (ZTE 2021). Major ZTE contracts include a US$82m construction project in 2002 for a rural telephone service in Nigeria and a US$95m follow-up for the second phase in 2005.

Table 2.1 Chinese companies supplying digital surveillance technologies

Supplier country: China			
Technology	**Supplier**	**Government**	**Examples**
Mobile interception	ZTE	Zambia	Via subsidiaries in Ghana, Nigeria, and Zambia – and also Côte d'Ivoire. Construction of a rural telephone service in Nigeria.
Internet interception			
Social media monitoring			
Smart cities	Huawei	Ghana, Malawi, Morocco, Nigeria, and Zambia. Also Côte d'Ivoire.	Huawei launched a US$1.5bn fund to support the development of smart cities across Africa; e.g. setting up digital infrastructure in Zambia where *The Wall Street Journal* reported it helped authorities intercept encrypted communications and use mobile data to track political opponents.
Biometric ID	Huawei and ZTE	Ghana	Ghana received a US$129m loan from China Exim Bank for extension of dedicated information infrastructure, including implementation of intelligent video surveillance by Huawei and ZTE.

Source: Authors' own. Created using data from Takouleu (2018); Ofori-Atta and Kan-Dapaah (2019); Parkinson *et al.* (2019a,b); Huawei (2020, 2021, 2022); ZTE (2021); Burkitt-Gray (2022); Abdulaziz (2023).

3. European Union

In the EU, exporting companies are expected to register sales of 'dual-use' equipment and are required to conduct human rights assessment to ensure that equipment they are exporting is not used to violate citizens' rights. Key European agencies are involved in the funding and coordination of the transfer of surveillance equipment (and associated training to use it), including the European Commission (EC), the European Border and Coast Guard Agency (Frontex), the European Union Agency for Law Enforcement Training (CEPOL), and the European External Action Service (EEAS). Two of these institutions – Frontex and the EEAS – are currently being investigated by the European Ombudsman over failures to conduct human rights assessments of their surveillance technology transfers to non-EU countries. A recent investigation into the EC by the European Ombudsman found that it had failed to ensure the protection of human rights in the transfer of surveillance technology to African governments (European Ombudsman n.d.).

Like China, the EU also uses soft loans to transfer technologies to the continent. This includes the Global Gateway Investment Package, which is focused on accelerating digital transformation through investments and is valued at €150bn (US$164bn) (EC n.d.b). It specifically aims to facilitate projects in fibre-optic cables, cloud computing, and data infrastructure.

The EU also controls the export, transit, brokering, and technical assistance of dual-use items. According to a September 2022 report prepared by the EC with input from member states in the Dual Use Coordination Group (DUCG), while it remains difficult to 'obtain reliable information on overall dual-use exports (including non-listed dual-use items) as there is no official category of "dual-use items" in official economic/trade statistics', the EC and member states collect some information that makes dual-use export estimations possible (EC 2022: 8). While the report – which includes data collected by member states from regulators and statistics for export declarations to EU customs – only provides aggregated export control data for 2020, it notes that 97 licences were granted for telecommunications and information security, 21 for computers, and 234 for electronics generally.

However, under the EU's dual-use export regulation, data about transfers are only offered to the EU by member states on a voluntary basis. On 24 January 2023, the EC's Directorate-General for Trade launched a consultation on new requirements for the collection and preparation of dual-use export data so the EU can more accurately report what is happening (EC n.d.a). Each member state's export licence authorities are subject to freedom of information legislation, meaning public access requests are an avenue for further investigation (EC 2022).

Border surveillance technologies

The EU has several funding mechanisms dedicated to border control and surveillance. Europe is engaged in a process of externalising[1] and digitalising its border control and surveillance, in part through programmes designed to provide technical and financial support to non-EU countries on migration issues. Such initiatives include the AENEAS Programme (EuropeAid 2008), the B7-667 budget line (EC 2002) and, most notably, the EU Trust Fund for Africa (EUTFA), which was established in 2015 to 'address the root causes of instability, forced displacement and irregular migration' (EUTF 2023).

A funding overview by NGO Statewatch highlights some of the projects funded via these mechanisms, breaking it down into three phrases: creating border infrastructure between 2001 and 2010; improving integration between 2011 and 2018; and the current phase of 'enhancing security', which began in 2018 and runs to the present (Statewatch 2019).

Significant EUTFA projects include:

- A €44m project titled 'Support for Integrated Border and Migration Management in Morocco' in 2018, which included the acquisition of equipment for the surveillance of sea and land borders, as well as improving use of data and cooperation with EU authorities. In 2019, the EC committed a further €101.7m to Morocco's border management, noting in a press release that it would include the use of 'new technologies' as well as 'analysis and collection of data on migration' (EC 2019).
- A €65m 'Border Management Programme for the Maghreb Region' which involves the transfer of equipment and training to Morocco between 2018 and 2024.
- A €15m project titled 'Dismantling the Criminal Networks Operating in North Africa and involved in Migrant Smuggling and Human Trafficking' to support 'the specialization of law enforcement agencies by establishing solid knowledge and skills on the use of special investigation techniques, including criminal intelligence analysis, forensics and digital forensics' (EUTF 2017).
- A €5m project for 'Strengthening Border Security in Ghana' designed to enhance the border checking and surveillance capacities of the Ghana Immigration Service (GIS).

[1] Border externalisation refers to the practice of outsourcing the responsibility for preventing migration to third countries and private entities.

Other avenues through which surveillance technologies are transferred to African governments include: the EU Agency for Law Enforcement Training (CEPOL), which facilitates training sessions for law enforcement officials throughout northern Africa, including Morocco (CEPOL 2020); and EU coastguard agency Frontex, which runs the Africa-Frontex Intelligence Community (AFIC) to conduct 'training and capacity building activities to develop national and regional strategies to fight cross-border crime and setting up integrated border management systems, as well as improving the collection, sharing and analysis of relevant data' in African countries, including Morocco, Ghana, and Nigeria (Frontex 2017).

A 2016 Joint AFIC report noted that the project has 'reached an enhanced level of maturity', which 'is mostly evident in the Community's capacity to generate analysis and knowledge, build trust between its participating partners, expand geographically and extend its product portfolio' (Frontex 2016: 8).

For Ghana specifically, it noted 'the authorities are addressing document and identity fraud by introducing biometric passports, birth and death certificates, and more effective arrest and prosecution of offenders' (*ibid*.: 30).

As part of a project launched under AFIC in 2017, Frontex is also helping Ghana and Nigeria set up Risk Analysis Cells, to 'collect and analyse strategic data on cross-border crime such as illegal border crossings, document fraud and trafficking in human beings' (Riehle 2019).

Member states: France, Germany, and Italy

Aside from surveillance transfers at the EU level, many EU member states have their own relationships and surveillance export arrangements with the five African countries.

France

France has a long colonial history of presence on the African continent and has maintained economic and political ties, including through military bases, control of monetary systems, and close trading relationships following a 'Françafrique' doctrine (Chrisafis 2023). Although French military presence may be reduced, increasing military training and equipment may signal a repacking of that doctrine (France24 2023). In the slipstream of French government politics come French surveillance technology companies that have hired former French officials to facilitate business in Francophone Africa (Braun 2022).

French technology transfers to Africa tend to be focused around signal intelligence technologies capable of intercepting mobile phone and internet data.

Founded in 2002, Altrnativ claims to have sold surveillance technologies to the governments of Benin, Chad, Cameroon, Comoros, Gabon, and the Republic of the Congo. One of the products offered by Altrnativ is their tailor-made search engine Targets. According to the company, this search service can retrieve publicly available data to analyse and identify connections between places, people, and organisations and thus provide information on people and their whereabouts.

Another French cyber-surveillance firm, Nexa Technologies, stated it had received permission from the French government and export licences for selling its surveillance software CEREBRO to repressive regimes such as the Egyptian government (Canet *et al*. 2021). CEREBRO provides real-time surveillance of the mobile phones of targeted citizens and the collection of personal data and metadata (Mada Masr 2021).

Germany

Germany is Europe's largest arms exporter and has at least 41 firms active in the high-tech surveillance industry (Privacy International 2016).

A company that has now shut operations and filed for bankruptcy was FinFisher. This surveillance technology company had a track record of selling to authoritarian regimes monitoring human rights defenders and journalists. Citizen Lab found evidence for the presence of FinFisher Command and Control servers in South Africa (Singh 2015). The company sold FinSpy, a 'surveillance software suite, capable of intercepting communications, accessing private data, and recording audio and video, from the computer or mobile devices it is silently installed on' (Amnesty International 2020). After years of public and legal pressure by non-governmental organisations (NGOs), the company was dissolved. It is worth mentioning that all staff moved to other technology firms and remain active in security or surveillance services (AccessNow 2022). The use of FinFisher's technology by state authorities has been documented in Nigeria and Morocco (Marczak *et al*. 2015).

Another German surveillance technology company is the Munich-headquartered Trovicor, which offers monitoring centres to government and law enforcement clients worldwide to capture, monitor, analyse, and store data from various networks (mobile and internet). The company, formerly part of Nokia Siemens Networks (NSN), delivered communications surveillance equipment to the Ethiopian government (Privacy International 2015a).

Italy

Italy has a large defence and security sector. In addition, the surveillance technology sector is growing, with over 20 active companies (Privacy International 2016). Historically, the Italian surveillance industry was fostered due to domestic demand for monitoring organised crime. The Italian Ministry of Economic Development (MISE), under Legislative Decree No. 221 of 2018 is tasked with granting export licences for dual-use technologies (TIMEP 2019).

Four companies seem often to be present in deals: AREA, RCS, SIO, and INNOVA, while others have resurfaced after scandals that involved them, such as Hacking Team, now active under the name of Memento Labs (Coluccini 2023). For example, the Moroccan intelligence services made use of Hacking Team's spyware Remote Control System and spent more than €3m on Hacking Team equipment (Privacy International 2015b). Other customers of this spyware were agencies of African governments of Egypt, Ethiopia, Morocco, Nigeria, and Sudan (Marczak *et al.* 2014).

Table 3.1 EU and EU member state companies supplying digital surveillance technologies

Supplier country: EU and member states France (F), Germany (DE), and Italy (IT)

EU institutions, Frontex, and the EEAS are being investigated by the European Ombudsman over failures to conduct human rights assessments of their surveillance technology transfers to non-EU countries

Technology	Supplier	Government	Examples
Mobile interception			
	Altrnativ (F)	Côte d'Ivoire	Deal worth €13.8m for radio surveillance equipment and intelligence training
	Nexa Technologies (F)	Egypt	Surveillance software CEREBRO, which provides real-time surveillance of the mobile phones of targeted citizens and the collection of personal data and metadata
	Finfisher (DE)	South Africa	FinFisher Command and Control servers in South Africa
	Hacking Team, now active under the name Memento Labs (IT)	Morocco	Moroccan intelligence services used spyware Remote Control System and spent more than €3m on Hacking Team equipment
Internet interception			
	Trovicor (DE)	Ethiopia	Communications surveillance equipment to the Ethiopian government
Social media monitoring			
	Altrnativ (F)	Multiple countries	Tailor-made search engine Targets, to retrieve publicly available data to analyse and identify connections between places, people, and organisations
Smart cities			
Biometric ID	EUTFA (EU)	Ghana	€5m project for 'Strengthening border security in Ghana' to enhance border checking and surveillance capacities of the Ghana Immigration Service
	EUTFA (EU)	Morocco	A €44m 'Support for integrated border and migration management in Morocco' project in 2018, including the acquisition of surveillance equipment for sea and land borders, as well as improving data use and cooperation with EU authorities

Source: Authors' own. Created using data from Marczak *et al.* (2014); Privacy International (2015a,b); Singh (2015); EUTF (2017); EC (2019); Canet *et al.* (2021); Mada Masr (2021); Braun (2022); Coluccini (2023); EUTF (2023).

4. Israel

In 2022, a consortium of journalists and civil society organisations revealed that Israeli Pegasus spyware was used to target some 50,000 journalists, human rights defenders, and foreign heads of state around the world (Amnesty International 2022). For Israel, the export of military-grade surveillance tools acts as a form of 'spyware diplomacy', providing a diplomatic bargaining chip for the country's political goals (Bergman and Mazzetti 2022; Dadoo 2022; Robinson 2022). The ongoing occupation of Palestine provides 'an open-air laboratory for Israel to test techniques of espionage and surveillance before selling them to repressive regimes around the world', states Dr Shir Hever, author of *The Privatisation of Israeli Security* (Shtaya 2022). These field-tested products are monetised via exports. The exported products and services cover a broad range from spyware and digital tools for surveillance to espionage, psychological operations, and disinformation (Loewenstein 2019, 2023).

In terms of its relationship to the African continent, prominent suppliers include Briefcam, whose 'video synopsis technology' has been incorporated into smart city surveillance networks in suburban areas throughout South Africa (Kwet 2019; Murray 2022); and Circles, a mobile interception firm, which is 'affiliated with NSO Group, which develops the often-abused Pegasus spyware' (Marczak *et al*. 2020: 1), and which is active in Botswana, Equatorial Guinea, Kenya, Morocco, Nigeria, Zambia, and Zimbabwe.

NSO Group itself is active in 45 countries worldwide, including Algeria, Egypt, Côte d'Ivoire, Kenya, Morocco, Rwanda, South Africa, Togo, Uganda, and Zambia (Mwesigwa 2019); while Team Jorge helped hack into the phones of opposition leaders during the 2015 Nigerian election.

The Israeli surveillance industry sees growth potential in the African market: 'African countries that have already bought Israeli security equipment represent a potential for further deals, such as the need to upgrade systems' (Salman 2021). 'The commercial aspect is an important driver for Israel's arms sales. The Israeli arms industry is extremely export dependent, and maintaining the industry is considered vital for both Israel's economy and security' interests, Wezeman (2011: 14) argues.

Dadoo (2022) argues that, 'For power-hungry African leaders looking to Israel as a blueprint for surveilling their own citizens, these technologies are ideal. They are relatively cheap, easily distributed and can be deployed with little consequences to their regimes.'

The country's 'military-innovation ecosystem' creates a continuous pipeline of surveillance tools which, according to Abdelnour (2023: 334), consists of a 'constellation of industries, infrastructures and organisations involved' in (digital) surveillance and 'weapons development, testing and sales'. This includes 'military and state agencies, tech start-ups and private companies, universities and research institutes, as well as banks and venture financing, including public research funding agencies for "dual-use" technologies' (*ibid.*).

In this ecosystem, the distinction between private and public space is blurred (Cook 2019), with former military personnel from Israel's cyber-surveillance units working for weapons companies and digital surveillance technology start-ups (Abdelnour 2023). US-based venture capital funds and technology firms are some of the biggest investors of Israeli surveillance firms (Kortum and Lerner 2000).

Table 4.1 Israeli companies supplying digital surveillance technologies

Supplier country: Israel			
Technology	**Supplier**	**Government**	**Examples**
Mobile interception			
	Circles	Morocco, Nigeria, and Zambia Also Botswana, Equatorial Guinea, Kenya, and Zimbabwe	
	NSO Group	Morocco, Nigeria, and Zambia Also Côte d'Ivoire, Egypt, Kenya, Rwanda, South Africa, Togo, and Uganda	Developers of the Pegasus spyware
	Team Jorge	Nigeria	Hacked into the phones of opposition leaders during the 2015 Nigerian election
Internet interception			
Social media monitoring			
Smart cities			
	Briefcam	South Africa	'Video synopsis technology' incorporated in smart city surveillance networks in suburban areas.
Biometric ID			

Source: Authors' own. Created using data from Kwet (2019); Mwesigwa (2019); Marczak *et al.* (2020); Murray (2022).

5. Russia

Like China, the EU, and the US, Russia is attempting to project its own influence over the African continent. Since 2015, for example, Russia has signed military-technical agreements with 21 African countries (Hedenskog 2018), including Nigeria (Ojoye 2021), Zambia, and Ghana, which allow for technology transfers. There is, however, no evidence of which surveillance technologies might be included in such agreements.

In June 2021, Russian state defence company Rosoboronexport – which sells a range of biometric identification technologies (Rosoboronexport 2021a) – announced it had signed contracts worth US$1.7bn with 17 sub-Saharan African countries (Rosoboronexport 2021b). While the press release does not mention which countries, the 'partner countries' section of its website notes that the company is known to have been cooperating with Nigeria since 1960 (Rosoboronexport 2023).

The main body in Russia responsible for export control over dual-use items is the Russian Federal Service for Technical and Export Controls (FSTEC), but it publishes no information on export licences granted. The Federal Service for Military-Technical Cooperation (FSVTS) also exists under the Ministry of Defence to manage military-technical cooperation with foreign states. While it does not publish information about technology exports or transfers, the director of the FSVTS noted in September 2018 that sub-Saharan African states have ordered US$3bn of military equipment from Russia (Interfax 2019).

According to the Stockholm International Peace Research Institute (Wezeman *et al*. 2021), Russia has supplied arms to 18 countries in sub-Saharan Africa over the past 10 years, including Ghana, Nigeria, and Zambia, although it is unclear whether any surveillance technologies were included in this.

However, World Bank data from 2020 shows that Russia's overall exports to sub-Saharan Africa are dwarfed by those from Germany, India, the US, and especially China (which accounted for 20.5 per cent of all imports into the region) (WITS 2019). In February 2023, the UK newspaper *Financial Times*, in a series on Russian involvement in the continent, also reported that 'Russia lacks the economic muscle to compete head-to-head with China, the US or EU when it comes to trade and investment in Africa' (Wilson 2023). Writing in October 2019 for the Carnegie Endowment for International Peace, Paul Stronski (2019) also noted that 'the modest size of Russia's technology sector and lack of investment resources hardly make it an attractive partner for African countries seeking to modernize or build new infrastructure'.

Despite this, a number of Russian companies are prominent in the surveillance technology space, particularly around Systems for Operative Investigative Activities (SORM), which refers to hardware and software that can intercept and monitor internet and telecommunications network traffic (Whittaker 2019). It is essentially the Russian equivalent of 'lawful interception' technology and was initially developed by the KGB in the mid-1980s during a project to intercept landline communications. SORM systems are now capable of targeted surveillance of specific individuals across the whole spectrum of internet and telephone communications technologies (see Box 5.1).

Box 5.1 What is a lawful interception technology?

The term 'lawful interception technologies' refers to the functionality that internet service providers and phone companies are required to build into their systems to allow surveillance that a court has warranted in accordance with legislation. A society may wish state agencies to conduct surveillance of the most serious criminals to prevent atrocities. Legislation can stipulate narrow circumstances in which this may take place, with democratic oversight and protection for the privacy of other citizens[1]. OpenDemocracy noted in 2012 that three SORM systems are currently in use which are capable of targeted surveillance of specific individuals across the whole spectrum of internet and telephone communications technologies (Soldatov and Borogan 2012).

However, there is very little open-source or public domain information about Russian SORM suppliers' involvement in supplying digital surveillance technologies to the five African countries that are part of this study: Nigeria, Ghana, Morocco, Malawi, and Zambia.

The chief commercial officer of Speech Technology Centre (STC) – a provider of facial, voice, and biometric identification systems – noted in 2016 that, 'Attention to biometric technologies on the African continent is raising rapidly', adding that 'South Africa and Nigeria are the key revenue generating countries in the African biometrics market' (Mayhew 2016).

[1] For more information on lawful interception, surveillance law, and how it can be subverted for unlawful interception, see Roberts *et al.* (2021).

Table 5.1 Russian companies supplying digital surveillance technologies

Supplier country: Russia			
Technology	**Supplier**	**Government**	**Examples**
Mobile interception			
Internet interception			
Social media monitoring			
Smart cities			
Biometric ID	Rosoboronexport	17 sub-Saharan African countries, including Nigeria	Signed contracts worth US$1.7bn

Source: Authors' own. Created using data from Hedenskog (2018); Ojoye (2021); Rosoboronexport (2021b).

6. United Kingdom

The UK has a long and brutal colonial history in Africa going back centuries. Some colonial surveillance systems, including those operated by the Special Branch, were adopted by post-independence governments and continue in modernised forms today. The UK government has also continued to have close political and economic ties with many of those governments, which has sometimes involved the transfer of surveillance equipment and training.

The easiest way to find data on these technology transfers is to look at the data regularly published by the Department for International Trade and the Export Control Joint Unit on the types of dual-use technologies being transferred overseas. This includes both quarterly and annual licensing statistics. This data can also be used to generate reports on, for example, specific licence types or export destinations, via a government portal.

By searching for specific 'control entries' related to the technologies being investigated by this project, we can see that the UK government greenlit the transfer of:

- 16 licences worth £669,880 to Malawi
- 79 licences worth £3,685,770 to Zambia
- 91 export licences worth £5,279,676 to Ghana
- 227 licences worth £49,176,911 to Morocco
- 572 licences worth £66,061,548 to Nigeria (DIT 2021).

The data here covers exports between 1 January 2013 and 1 February 2023, which were the furthest and most recent dates the function would allow. The licences granted specifically allow for the transfer of drones, camera equipment (6A003), telecommunications interception software and equipment, internet protocol (IP) network surveillance, various forms of cryptography, and information security technologies.

In terms of overall exports, however, Africa generally represents only a fraction of the total. The most recent UK defence and security exports data (GOV.UK n.d.b), for example, shows that between 2012 and 2021, Africa as a region accounted for just 1 per cent of UK defence exports (GOV.UK n.d.a). Technology transfers are included in this data.

Comparing this to data collected via freedom of information (FOI) by Campaign Against the Arms Trade (CAAT n.d.), the total value of dual-use goods (including those not specifically related to digital surveillance technologies) exported to each country since 2008 are as follows:

- Malawi, £789,000
- Zambia, £4.7m
- Ghana, £36m
- Morocco, £115m
- Nigeria, £348m

However, while the UK government openly publishes more dual-use export licensing data than many other governments, there are still severe limitations in the level of detail and transparency the data provides. For example, it does not show whether the goods were actually exported, only that the licence holder has been permitted to export them; and it does not disclose specific suppliers or technologies. More information can be gathered about suppliers through FOI requests.

An FOI from Motherboard in 2016, for example, found that companies involved in transferring surveillance technology include the billion-dollar arms exporter BAE Systems, as well as Pro-Solve International, ComsTrac, CellXion, Cobham, and Domo Tactical Communications (DTC) (Cox 2016). Motherboard noted that 33 licences were explicitly marked as being for IMSI catchers (see Box 6.1). While all these firms are UK-based, DTC is headquartered in the US. According to a joint investigation by BBC Arabic and the Scandinavian newspaper *Dagbladet* from 2017, BAE Systems has sold a mobile and internet interception system called Evident (developed by a firm called ETI that BAE purchased in 2011) to authorities in Morocco, as well as Saudi Arabia, the UAE, Qatar, Oman, and Algeria (BBC 2017). An anonymous former employee of ETI told the BBC:

> [With Evident], *you'd be able to intercept any internet traffic. If you wanted to do a whole country, you could. You could pin-point people's location based on cellular data. You could follow people around. They were quite far ahead with voice recognition. They were capable of decrypting stuff as well.*
> (BBC 2017)

Box 6.1 Explainer: What is an IMSI catcher?

An IMSI catcher is a surveillance technology that allows users to hack into mobile phone traffic (calls, text messages, instant messaging, and anything sent from your mobile phone). The hacker catches this data by imitating a mobile phone cell tower to intercept the data. The hacker can catch mobile data without the knowledge of the caller and without needing access to the handset. Note that the IMSI equipment is sometimes called a Stingray and the type of hack is often referred to as a man-in-the-middle attack. IMSI stands for International Mobile Subscriber Identity: an identifier unique to each mobile phone that is used to identify it to cell towers. Any single phone is constantly sending out signals to find the nearest cell tower to optimise signal strength and identify itself – and this provides the opportunity for the hack to imitate a cell tower and catch the phone's data.

A follow-up report from Motherboard in 2018 noted that the UK government has since been reluctant to release information about suppliers, claiming the information needs to be protected for 'commercial interests' (Cox 2018).

Table 6.1 UK companies supplying digital surveillance technologies

Supplier country: UK			
Technology	**Supplier**	**Government**	**Examples**
Mobile interception **Internet interception**	ETI (purchased by BAE)	Morocco, also Algeria, Qatar, Oman, Saudi Arabia, and the UAE	Mobile and internet interception system called Evident
Social media monitoring			
Smart cities			
Biometric ID		Ghana and Nigeria, also Côte d'Ivoire	Border and coastal surveillance

Source: Authors' own. Created using data from BBC (2017).

7. United States of America

There are 122 surveillance companies headquartered in the US. Due to the vast apparatus of US secret service, domestic intelligence, and security agencies, a large domestic market for surveillance technology fosters an ecosystem of surveillance companies (Privacy International 2016). US companies supply AI-related surveillance technologies to at least 32 countries worldwide, the most significant being IBM, Palantir, Clearview AI, Clarifai, Intel, and Cisco (Feldstein 2019; Peterson and Hoffman 2022). According to Feldstein (2019), the most significant US exporters worldwide are IBM (11 countries), Palantir (nine countries), and Cisco (six countries), but they have been eclipsed in Africa by China's Huawei and ZTE (see China section of this report). In the safe city market for urban surveillance systems, US company Honeywell has advanced projects in Bangaluru, India, and Cairo, Egypt, but it is again China's Huawei and ZTE who look like dominating the African market with large projects in Ghana, Malawi, and Zambia (see those country reports in this publication).

Although not related to governmental use of data collection or surveillance, the United Nations (UN) World Food Programme (WFP) agreement with Palantir for biometric data collection may affect migrants and refugees in Africa. 'Data collection is not an apolitical exercise, especially when powerful global North actors collect information on vulnerable populations with no regulated methods of oversights and accountability', states UN special rapporteur on racism, racial discrimination, xenophobia, and related intolerance Professor Tendayi Achium (Klovig Skelton 2020). International aid funds are used to increase the digital surveillance of migrants and refugees.

US companies are also active in social media surveillance. Dataminr, for example, specialises in advanced real-time social media monitoring and provides the UN with its First Alert service to alert first responders on breaking news (Dataminr 2023). The company has also helped US law enforcement agencies track protests (Levin 2016) and public authorities in South Africa to monitor student demonstrations in Cape Town (Dataminr 2016). Dataminr's customers in Africa also include governmental agencies in Kenya (used during the 2017 elections) and Nigeria (Thorpe 2019). *The Intercept* reports:

> And despite Dataminr's claims that its law enforcement service merely 'delivers breaking news alerts on emergency events, such as natural disasters, fires, explosions and shootings,' as a company spokesperson said, the company has facilitated the surveillance of protests, including nonviolent activity, siphoning vast amounts of social media data from

> across the web and converting it into tidy police intelligence packages. (Biddle 2020)

The US Department of Commerce's Bureau of Industry and Security oversees the licensing of export of surveillance technologies (Export Controls Act of 2018), while the departments of Commerce, Defense, State, and Energy may approve or deny a licence as long as it is 'consistent with national security and foreign policy interests' (TIMEP 2019).

Collaboration between state actors and private partners is increasing. The US, 'Big Tech', and the US military apparatus are increasingly intertwined in research, development, and delivery of surveillance products and services and using them for geopolitical goals (González 2023). Similar patterns can be recognised in their adversarial counterparts.

Despite the sheer size, the US surveillance companies are less visible than other countries' suppliers across the African countries investigated for this ADRN study. However, as Duncan (2018) argues, surveillance is a serious issue on the African continent, and the US has been actively developing the internet as a global spy machine for its own interests. This has led to other countries challenging that hegemony and pursuing different governance of the internet and their own surveillance interests.

Table 7.1 US companies and UN entities supplying digital surveillance technologies

Supplier country: USA (and UN entities)			
Technology	**Supplier**	**Government**	**Examples**
Mobile interception	Israeli branch of US-based Verint Systems	South Sudan	Surveillance equipment to intercept communication
Internet interception			
Social media monitoring	Dataminr	Nigeria Also Kenya and South Africa	Monitoring student demonstrations in Cape Town, South Africa
Smart cities	Honeywell	Egypt	Surveillance systems for large smart city projects
Biometric ID	Palantir	UN World Food Programme	International aid funds are used for digital surveillance of migrants and refugees

Source: Authors' own. Created using data from Dataminr (2016); Thorpe (2019); Feldstein (2019); Biddle (2020); Peterson and Hoffman (2022).

8. Conclusion

1. This is a global industry facilitated by governments of competing rich countries, and African governments are buying from all of them with little regard for their geopolitical rivalries.
2. Publicly available information from governments and suppliers is superficial. While it will show that surveillance transfers are taking place, most detail can be found in investigative reports by journalists and NGOs. Even governments that do provide a higher degree of insight into their transfers, like the UK, still operate their export regimes with a high level of opacity. Most offer no meaningful insights.
3. China is by far the most scrutinised exporting country when it comes to volume of research on its surveillance transfers. Equivalent research scrutiny is not being applied to the USA, their main competitor, or others, despite the same perils to human rights.
4. Surveillance technologies are being transferred, but the surveillance element is being downplayed. For example, the EU's transfers are often under the guise of helping African states manage migration, while smart city technologies are pitched by suppliers as a way of boosting the local economy or administering local government functions, i.e. the stated purpose is not surveillance, even though the capabilities are provided.

African governments are not discriminating between competing powers when accepting surveillance technology, and all of these powers are engaged in providing it. We also note that suppliers themselves may not distinguish their customers based on geopolitical alliances and they sell to non-allied or adversarial countries (DeSombre, Gjesvik and Ole Willers 2021). Israeli firm Cellebrite, for example, despite being headquartered in a country with strong links to the US and NATO, regularly sells to Russian and Chinese buyers. Another example is Swedish mobile forensic software company MSAB, which also markets to Russian and Chinese buyers despite being in an EU/NATO country.

While many technology firms do not sell surveillance equipment directly, they do supply technology and services that have the capacity to be used for surveillance.

Looking at the exporting governments, Russia is a massive global arms exporter, but there is little evidence to suggest it is a major supplier of digital surveillance technologies to African states. Even though the Russian state has the capacity to supply these technologies, its counterparts from the US, China, and Europe are far more active in this regard. There is evidence, however, that Russia is supplying these technologies elsewhere, particularly in Central Asia (Bourgelais 2013).

Given China's growing geopolitical significance, there has also been significantly more research conducted into its technology exports than other governments. The scale of China's investment on the continent, however, and its advanced technology sector, with at least dozens of active firms, means further research is needed to fully understand the web of actors involved.

Further research is also particularly needed into EU surveillance technology transfers, which are carried out by a complex web of institutions at both the supranational and national levels, as well as those from the UK which, while providing a higher level of transparency than other governments, does not provide any public information on exact technologies or suppliers. More research is also needed into specific member states' technology transfers; something we could not fully cover given the number of countries involved and lack of transparency in many, which necessitates alternative, more time-consuming research methods.

The EU is currently in the process of updating its export licence controls, which could potentially mandate greater transparency around dual-use exports, opening up further avenues of research into both the bloc and specific member states.

In terms of the specific technologies being transferred, each exporting country tends to have a focus area, at least within the five technology types covered by this report. The UK, for example, is involved in the transfer of mobile and internet interception technology, but not the provision of biometric ID or smart city technologies.

Exporting governments also tend to be focused on particular countries, even if some, like the UK and China, are active in all of them. The EU, for example, is heavily involved in Morocco and other North African countries, but it is much less involved in Malawi and Zambia. China, on the other hand, is active in Morocco but to a much lesser extent than it is in Nigeria and Ghana.

Table 8.1 Summary of suppliers of digital surveillance technologies to African countries by country

China	China is a major and growing supplier of digital surveillance technologies, particularly those that use AI. Many of the loans provided by China to African countries are for IT infrastructure projects, rather than direct surveillance capabilities, although many of the technologies being transferred could be repurposed for surveillance.
EU	Like China, the EU and its agencies use foreign investment mechanisms to transfer technologies to Africa. Aside from surveillance transfers at the EU level, many member states have their own relationships and surveillance export arrangements with the five countries covered in this report, including Germany, France, and Italy.
Israel	Israel's 'military-innovation ecosystem' creates a continuous pipeline of surveillance tools. In this ecosystem, the distinction between private and public space is blurred.
Russia	Russia is attempting to project its influence over Africa, but there is little evidence to suggest it is a major supplier of digital surveillance technologies to African states.
UK	The UK government has close political and economic ties with many of the former African colonies. This has sometimes involved the transfer of surveillance equipment and training.
USA	There are over 120 surveillance companies headquartered in the US. The US government agencies, 'Big Tech', and the US military apparatus are increasingly intertwined in research, development, and delivery of surveillance products and services and are using them for geopolitical goals.

Source: Authors' own.

References

Abdelnour, S. (2023) '**Making a Killing: Israel's Military-Innovation Ecosystem and the Globalization of Violence**', *Organization Studies* 44.2: 333–37 DOI: 10.1177/01708406221131938 (accessed 11 August 2023)

Abdulaziz, I. (2023) '**With Kano Centre, Nigeria Pushes For Data Sovereignty, Better Security**', *NAN News*, 15 February (accessed 12 May 2023)

AccessNow (2022) '**Victory! FinFisher Shuts Down**', press release, 29 March (accessed 12 May 2023)

AidData (n.d.) ***Project ID: 30956. China Eximbank Provides $123.4 Million Preferential Buyer's Credit for Phase 2 of Dedicated Security Information System Project (Linked to #1862)*** (accessed 12 May 2023)

Amnesty International (2022) ***The Pegasus Project: How Amnesty Tech Uncovered the Spyware Scandal – New Video***, 23 March (accessed 12 May 2023)

Amnesty International (2020) ***German-Made FinSpy Spyware Found in Egypt, and Mac and Linux Versions Revealed***, 25 September (accessed 12 May 2023)

BBC (2017) ***How BAE Sold Cyber-Surveillance Tools to Arab States***, 15 June (accessed 12 May 2023)

Bergman, R. and Mazzetti, M. (2022) '**The Battle for the World's Most Powerful Cyberweapon**', *The New York Times*, 28 January (accessed 12 May 2023)

Biddle, S. (2020) '**Police Surveilled George Floyd Protests with Help from Twitter-Affiliated Startup Dataminr**', *The Intercept*, 9 July (accessed 12 May 2023)

Boston University Global Development Policy Center (2022) ***Chinese Loans to Africa Database*** (accessed 12 May 2023)

Bourgelais, P. (2013) ***Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia, Access*** (accessed 12 May 2023)

Braun, E. (2022) '**Destination Africa: The Scramble to Sell Cyberweapons to Dictators**', *Politico*, 7 December (accessed 12 May 2023)

Burkitt-Gray, A. (2022) '**Malawi Government Sets Up National Data Centre with Huawei**', *Capacity*, 26 July (accessed 12 May 2023)

CAAT (n.d.) ***UK Export Licences Approved for Dual-Use Goods Since 2008***, Campaign Against Arms Trade (accessed 12 May 2023)

Canet, J-P.; Destal, M.; Labed, R.; Lavrilleux, A. and Livolsi, G. (2021) '**Surveillance Made in France**', *Egypt Papers*, 23 November (accessed 12 May 2023)

CEPOL (2020) ***EUROMED Police***, European Union Agency for Law Enforcement (accessed 12 May 2023)

China Daily (2022) '**Huawei-Supported 5G Network Launched in Zambia**', 26 November (accessed 12 May 2023)

Chrisafis, A. (2023) '**Macron Pledges to Reduce French Military Presence in Africa**', *The Guardian*, 27 February (accessed 12 May 2023)

Coluccini, R. (2023) '**Gli Spyware Italiani sul Mercato Internazionale**', *RPI Media*, 8 February (accessed 12 May 2023)

Cook, J. (2019) '**Israeli Spyware Technology, Tested on Palestinians, Now Operating in a City Near You**', *Washington Report on Middle East Affairs*, 9 December (accessed 12 May 2023)

Cox, J. (2018) '**UK Government is Cozy with Companies Selling Spytech**', *Vice*, 17 April (accessed 12 May 2023)

Cox, J. (2016) '**British Companies Are Selling Advanced Spy Tech to Authoritarian Regimes**', *Vice*, 26 August (accessed 12 May 2023)

Dadoo, S. (2022) '**Israel's Spyware Diplomacy in Africa**', *Orient XXI*, 12 September (accessed 12 May 2023)

Dataminr (2023) ***Real-Time Alerts Inform UN Response and Humanitarian Aid Delivery***, First Alert (accessed 12 May 2023)

Dataminr (2016) ***Product Update: Geospatial Analysis Application*** (accessed 30 May 2023)

DeSombre, W.; Gjesvik, L. and Ole Willers, J. (2021) ***Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets***, Washington DC: Atlantic Council (accessed 12 May 2023)

DIT (2021) ***UK Strategic Export Controls***, London: Department for International Trade (accessed 12 May 2023)

Duncan, J. (2018) '**Taking the Spy Machine South: Communications Surveillance in Sub-Saharan Africa**', in B. Mutsvairo (ed.), *The Palgrave Handbook of Media and Communication Research in Africa*, Cham: Palgrave Macmillan (accessed 12 May 2023)

EC (n.d.a) ***Guidelines for Data Collection and Preparation of the EU Annual Report on Dual-Use Export Controls Under Regulation (EU) 821/2021***, European Commission (accessed 12 May 2023)

EC (n.d.b) ***EU-Africa: Global Gateway Investment Package***, European Commission (accessed 12 May 2023)

EC (2022) ***Cover Note: Report from the Commission to the European Parliament and the Council on the Implementation of Regulation (EU) 2021/821 Setting Up a Union Regime for the Control of Exports, Brokering, Technical Assistance, Transit and Transfer of Dual-Use Items***, European Commission (accessed 12 May 2023)

EC (2019) '**The EU is Boosting its Support to Morocco with New Programmes Worth €389 Million**', *European Commission*, press release, 20 December (accessed 30 May 2023)

EC (2002) '**European Commission: Integrating Migration Issues into the EU's External Relations**' *European Commission*, press release, 3 December (accessed 12 May 2023)

EuropeAid (2008) ***Aeneas Programme: Programme for Financial and Technical Assistance to Third Countries in the Area of Migration and Asylum. Overview of Projects funded 2004–2006***, European Commission (accessed 12 May 2023)

European Ombudsman (n.d.) '**Decision on How the European Commission Assessed the Human Rights Impact Before Providing Support to African Countries to Develop Surveillance Capabilities (Case 1904/2021/MHZ)**', (accessed 12 May 2023)

EUTF (2023) ***Emergency Trust Fund for Africa: Sahel and Lake Chad***, European Union, Trust Fund for Africa (accessed 12 May 2023)

EUTF (2017) ***Dismantling the Criminal Networks Operating in North Africa and Involved in Migrant Smuggling and Human Trafficking***, European Union Trust Fund for Africa (accessed 30 May 2023)

Feldstein, S. (2019) *The Global Expansion of AI Surveillance*, Washington DC: Carnegie Endowment for International Peace

France24 (2023) '**France Must Demonstrate "Profound Humility" Towards Africa, Macron Says Ahead of Four-Nation Trip**', 27 February (accessed 16 May 2023)

Frontex (2017) ***Strengthening of AFIC as an Instrument to Fight Serious Cross-Border Crimes Affecting Africa and the EU***, Warsaw: Frontex (accessed 11 August 2023)

Frontex (2016) ***Africa-Frontex Intelligence Community Joint Report***, Warsaw: Frontex (accessed 16 May 2023)

Gagliardone, I. (2020) '**The Impact of Chinese Tech Provision on Civil Liberties in Africa**', *Policy Insights* 99: 1–20 (accessed 16 May 2023)

González, R.J. (2023) '**Militarising Big Tech: The Rise of Silicon Valley's Digital Defence Industry**', *TNI*, 7 February (accessed 16 May 2023)

GOV.UK (n.d.a) ***UK Defence and Security Exports for 2021*** (accessed 16 May 2023)

GOV.UK (n.d.b) ***Chart 7: Total UK Defence Exports (Based on Orders/Contracts Signed) by Region 2012 to 2021*** (accessed 16 May 2023)

Hedenskog, J. (2018) ***Russia is Stepping Up its Military Cooperation in Africa***, FOI Memo 6604, Stockholm: Swedish Defence Research Agency (accessed 16 May 2023)

Huawei (2022) ***New ICT Helps Build Smart Zambia*** (accessed 16 May 2023)

Huawei (2021) ***West Africa's CloudExchange Rapidly Transforms into a Leading ISP with Huawei*** (accessed 16 May 2023)

Huawei (2020) ***Ghana Commercial Bank Implements a Mobile Money Strategy*** (accessed 16 May 2023)

Interfax (2019) ***РФ анонсировала новые соглашения о военном сотрудничестве со странами Африки*** [Russia Announces New Agreements on Military Cooperation with African Countries] (accessed 16 May 2023)

Klovig Skelton, S. (2020) 'Humanitarian Data Collection Practices Put Migrants at Risk', *Computer Weekly*, 13 November

Kortum, S. and Lerner, J. (2000) '**Assessing the Contribution of Venture Capital to Innovation**', *RAND Journal of Economics* 31.4: 674–92, DOI: 10.2307/2696354 (accessed 16 May 2023)

Kwet, M. (2019) '**Smart CCTV Networks Are Driving an AI-Powered Apartheid in South Africa**', *Vice*, 22 November (accessed 16 May 2023)

Levin, S. (2016) '**Twitter Blocks Government "Spy Centers" From Accessing User Data**', *The Guardian*, 15 December (accessed 16 May 2023)

Loewenstein, A. (2023) *The Palestine Laboratory: How Israel Exports the Technology of Occupation Around the World*, London: Verso Books

Loewenstein, A. (2019) '**Exporting the Technology of Occupation**', *The New York Review*, 4 January (accessed 16 May 2023)

Mada Masr (2021) 'French Tech Executives Indicted After Selling Surveillance Software to Libya, Egypt', 23 June

Marczak, B.; Guarnieri, C.; Marquis-Boire, M. and Scott-Railton, J. (2014) ***Mapping Hacking Team's 'Untraceable' Spyware***, Citizen Lab, 17 February (accessed 16 May 2023

Marczak, B.; Scott-Railton, J.; Rao, S.P., S.; Anstis, S. and Deibert, R. (2020) ***Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles***, Citizen Lab Research Report 133, Toronto: University of Toronto (accessed 16 May 2023)

Marczak, B.; Scott-Railton, J.; Senft, A.; Poetranto, I. and McKune, S. (2015) *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation*, Citizen Lab Research Report 64, Toronto: University of Toronto

Mayhew, S. (2016) '**STC Demos Latest Multimodal Biometric Solutions at Africa Aerospace and Defence Expo**', *BiometricUpdate.com*, 27 September (accessed 16 May 2023)

Murray, M. (2022) *The Infrastructures of Security: Technologies of Risk Management in Johannesburg*, Ann Arbor MI: University of Michigan Press

Mwesigwa, D. (2019) ***Africa in the Crosshairs of New Disinformation and Surveillance Schemes That Undermine Democracy***, CIPESA blog, 9 December (accessed 16 May 2023)

Nedopil, C. (2023) *Countries of the Belt and Road Initiative*, Shanghai: Green Finance & Development Center (accessed 17 May 2023)

Ofori-Atta, K. and Kan-Dapaah, A. (2019) ***Joint Memorandum for the Approval of the Commercial Contract, Facility Agreement and Tax Exemption for the Implementation of the Integrated National Security Communications Enhancement (ALPHA) Project (Phase 11)***, Accra: Parliament of Ghana Library (accessed 17 May 2023)

Ojoye, O. (2021) '**Nigeria Signs Military-Technical Cooperation Agreement with Russia**', Ministry of Defence, Federal Republic of Nigeria, press release, 29 August (accessed 17 May 2023)

Parkinson, J.; Bariyo, N. and Chin, J. (2019a) '**Huawei Technicians Helped African Governments Spy on Political Opponents**', *The Wall Street Journal*, 15 August (accessed 17 May 2023)

Parkinson, J.; Bariyo, N. and Chin, J. (2019b) ***The Wall Street Journal Claims Huawei Technologies Staff Helped Zambia & Uganda Govts. Spy on Opponents; Company Denies Allegations***, Business & Human Rights Resource Centre, 15 August (accessed 17 May 2023)

Peterson, D. and Hoffman, S. (2022) *Geopolitical Implications of AI and Digital Surveillance Adoption*, Brookings Institution Policy Brief, Washington DC: Brookings Institution

Privacy International (2016) ***The Global Surveillance Industry***, July (accessed 17 May 2023)

Privacy International (2015a) ***Ethiopia Expands Surveillance Capacity with German Tech Via Lebanon***, 23 March (accessed 17 May 2023)

Privacy International (2015b) ***Facing the Truth: Hacking Team Leak Confirms Moroccan Government Use of Spyware***, 10 July (accessed 17 May 2023)

Riehle, C. (2019) '**Risk Analysis Cell in Niger**', *Eucrim*, 18 February (accessed 17 May 2023)

Roberts, T.; Mohamed Ali, A.; Farahat, M.; Oloyede, R. and Mutung'u, G. (2021) ***Surveillance Law in Africa: A Review of Six Countries***, Brighton: Institute of Development Studies, DOI: **10.19088/IDS.2021.059** (accessed 17 May 2023)

Robinson, K. (2022) ***How Israel's Pegasus Spyware Stoked the Surveillance Debate***, Council on Foreign Relations, 8 March (accessed 17 May 2023)

Rosoboronexport (2023) ***Partner Countries and Joint Projects*** (accessed 17 May 2023)

Rosoboronexport (2021a) ***Forensic Equipment*** (accessed 17 May 2023)

Rosoboronexport (2021b) **'Rosoboronexport Increased its Order Portfolio in Sub-Saharan Africa by $1.7 Billion**', press release, 7 June (accessed 17 May 2023)

Salman, Y. (2021) 'The Security Element in Israel-Africa Relations', *Strategic Assessment* 24.2: 38–53

Shtaya, M. (2022) ***Nowhere to Hide: The Impact of Israel's Digital Surveillance Regime on the Palestinians***, Middle East Institute, 27 April (accessed 30 May 2023)

Singh, A. (2015) ***FinFisher Research Referenced in Articles on German Court Investigation, South African Servers***, Citizen Lab, 25 February (accessed 17 May 2023)

Soldatov, A. and Borogan, I. (2012) '**Project_ID: Who's Bugging the Russian Opposition?**', *Open Democracy*, 24 February (accessed 17 May 2023)

Statewatch (2019) ***Aid, Border Security and EU-Morocco Cooperation on Migration Control***, 24 November (accessed 17 May 2023)

Stronski, P. (2019) ***Late to the Party: Russia's Return to Africa***, Washington DC: Carnegie Endowment for International Peace (accessed 17 May 2023)

Takouleu, J.M. (2018) '**AFRICA: Huawei Sets Up a $1.5 Billion Fund to Boost African Smart Cities**', *Afrik21*, 6 June (accessed 17 May 2023)

Thorpe, J. (2019) '**ISJ Exclusive: Be Ready for Anything with Dataminr**', *International Security Journal*, 14 November (accessed 17 May 2023)
TIMEP (2019) ***TIMEP Brief: Export of Surveillance to MENA Countries***, Tahrir Institute for Middle East Policy, 23 October (accessed 17 May 2023)

Wezeman, S.T. (2011) ***Israeli Arms Transfers to Sub-Saharan Africa***, SIPRI Background Paper, Solna: Stockholm International Peace Research Institute (accessed 17 May 2023)

Wezeman, P.D.; Kuimova, A. and Wezeman, S.T. (2021) ***Trends in International Arms Transfers***, SIPRI Fact Sheet, Solna: Stockholm International Peace Research Institute (accessed 17 May 2023)

Whittaker, Z. (2019) '**Documents Reveal How Russia Taps Phone Companies for Surveillance**', *TechCrunch*, 18 September (accessed 17 May 2023)

Wilson, T. (2023) 'Russia's Growing Trade in Arms, Oil and African Politics', *Financial Times*, 14 February

WITS (2019) ***Sub-Saharan Africa Imports, Tariffs by Country and Region 2020***, World Integrated Trade Solution (accessed 17 May 2023)

Woodhams, S. (2020) '**China, Africa, and the Private Surveillance Industry**', *Georgetown Journal of International Affairs* 21: 158–65 (accessed 17 May 2023)

ZTE (2021) '**Announcement: Provision of Performance Guarantee Limits for Overseas Subsidiaries for 2021**', Overseas Regulatory Announcement, ZTE Corporation (accessed 17 May 2023)