PRIVACY INTERNATIONAL

Teach ‘em to Phish: State Sponsors of Surveillance



July 2018

“The most significant human rights issues included: an incident of forced disappearance; abusive and degrading treatment by security officials that in some cases led to death; the use of caning as a legal punishment; indefinite detention without warrant or judicial review for persons suspected of certain security-related crimes; arbitrary arrest and detention of government critics; limits on the freedoms of expression, including for the press, assembly, and association; limits on political rights and privacy.”[1]

- Malaysia Human Rights Report,
  United States Department of State, 2017

“We only knew how to use Google to get evidence and information, but after the first day here, I learned from the FBI agents how to use different tools and devices to find other activities, which are linked together… I called my team that night and told them about these new devices, and I just heard from them that the results were tremendous.”[2]

- Ravindar Singh, Assistant Director of the Narcotics Intelligence Division, Royal Malaysia Police, 2017

Privacy International would like to thank Tim Shorrock for his contribution to this report.

Contents

Executive Summary	04
Introduction: From Military Aid to Security Assistance	06
What it Looks Like Now: Law Enforcement and Military Security Assistance	07
United States	07
Department of State	07
Department of Defense	10
Department of Justice	13
Schools of Surveillance	13
Use of Contractors	15
US-Funded Training in Intelligence, Surveillance and Reconnaissance (ISR)	20
Europe	23
European Union	23
Diversion of Development Funds	26
European Countries	27
China	29
What We Aren’t Permitted to Know: Intelligence Agencies Assistance	31
Conclusion - Assisting Human Security	33

Cover image courtesy of Unsplash / Icons & graphics courtesy of Flaticon.com

Executive Summary

Countries with the most extensive security and military agencies are transferring electronic surveillance capabilities, practices, and legislation around the world. They’re doing it by training foreign personnel, donating and providing loans for equipment, and directly financing security and military agencies. It’s happening through security cooperation agreements, development assistance, and security sector reform programmes. Implementation involves numerous donors, international organisations, countries, government agencies and departments, implementing partners, and contractors.

Assistance can reinforce authoritarianism, undermine governance, facilitate corruption, can illegitimately equip non-state actors, and exacerbate inter-communal tensions.

While such cooperation and assistance can strengthen security capacity in recipient states, there are also huge risks. As more data is being generated and as surveillance technology advances ahead of laws sufficiently regulating them, and while authoritarian leaders continue to use surveillance as tools of political control, such transfers pose a substantial threat to human rights around the world. Many of the recipient countries and agencies have a documented history of human rights abuses, meaning that in many cases, without appropriate safeguards and accountability, such assistance can facilitate gross abuses - something recognised by the US Government Accountability Office[3] and by a UK Parliamentary Home Affairs Committee.[4] Assistance can reinforce authoritarianism,[5] undermine governance,[6] facilitate corruption,[7] can illegitimately equip non-state actors, and exacerbate inter-communal tensions.[8]

Military and security capabilities proliferated worldwide during the Cold War era because of military assistance programmes and state support of a defence and security industry in large arms exporting states. As well as facilitating security cooperation and giving them political influence, such cooperation played, and continues to play, a defining role in maintaining the ability of recipient governments to exercise functions of the state and political control. Technological developments and a new security climate has meant that electronic surveillance used to identify and monitor people, their movement, their internet activity, and their electronic devices has become an established and ever-increasing internal security practice. As a result, surveillance for internal security purposes has been incorporated into these foreign security assistance programmes. In 2001, the US spent $5.7 billion in security aid – in 2017 it spent over $20 billion.[9] In 2015, military and non-military security assistance in the US amounted to an estimated 35% of its entire foreign aid expenditure.[10]

In 2001, the US spent $5.7 billion in security aid – in 2017 it spent over $20 billion. In 2015, military and non-military security assistance in the US amounted to an estimated 35% of its entire foreign aid expenditure. At the same time, developed countries and institutions such as the European Union (EU) are spending billions of Euros transferring surveillance and border control capabilities to foreign countries to ensure they stop people migrating to their countries.

At the same time, developed countries and institutions such as the European Union (EU) are spending billions of Euros transferring surveillance and border control capabilities to foreign countries to ensure they stop people migrating to their countries. The number of forcibly displaced people around the world is at a record high: in 1997 there were 33.9 million people displaced as a result of persecution, conflict, violence, or human rights violations; in 2016 there were 65.6 million.[11] 84% of the world’s refugees are being hosted in developing regions, with the least developed countries providing asylum to 28 per cent of the global total.[12] The EU and individual European countries are sponsoring surveillance globally to ensure that developing countries continue to host the vast majority of people forcibly displaced. Not only have such policies facilitated human rights abuses, they have allowed authoritarian and even genocidal leaders to use migration to gain political and economic support.[13] To fund this securitisation of foreign countries, donor countries are repurposing development funding for surveillance, border control, military and other ‘security’ spending.[14]

Such securitisation is hugely appealing for industry, allowing security companies and contractors to benefit from increased sales of security equipment, training contracts, and increased public financial support for the research and development of their products. Contractors are deeply involved in the delivery of surveillance training programmes around the world.

This report outlines the varying forms of foreign security assistance by law enforcement, military, and intelligence agencies. These examples show how specific programmes and agencies drive and advance the capabilities of other government agencies around the world. As such assistance involves the engagement of security actors, it offers a powerful mechanism through which to safeguard surveillance practices in recipient states by improving governance, rule of law, and adherence to human rights standards. Recommendations to this end are provided in the conclusion.

Introduction: From Military Aid to Security Assistance

The projection of soft and hard power throughout the Cold War saw the formation of military and intelligence alliances as well as the large-scale transfer of military and intelligence capabilities from hegemonic and colonial states to allied, non-aligned, and postcolonial states. The provision of military aid - key to the development of military alliances[15] - was a central foreign policy instrument for the US and Soviet Union: not only did it consolidate the domestic power of favourable regimes and strengthen their military capabilities, it also allowed them to leverage considerable political influence over them, obtain political favours, and covertly deliver military equipment to allied regional non-state actors.[16] The colonial European powers, in entrenched positions of influence in colonies, developed similar assistance programmes with newly liberated states beginning initially in the late colonial period with the establishment of independent security and military institutions.[17]

At the same time, the increasing prevalence of digital and computerised systems saw their wide use for a range of internal security purposes, including surveillance devices and computerised identification systems – the trade in which was dubbed the International Repression Trade in 1979 by Michael Klare.[18] While in-depth data about the extent of the trade in these capabilities was lacking at the time, the examples available showed transfers - generally mandated or at least supported by policy in the exporting government - overwhelmingly originating in industrialised and hegemonic states to allied countries in the global South.[19]

During the Cold War, for example, US security assistance programs led to the provision of internal security equipment and other assistance to a wide range of allied countries, including Nicaragua, the Philippines, and Thailand.[20] Similarly, the Israeli government provided counter-insurgency advisors and other assistance to the Guatemalan government during the civil war.[21]

While espionage and state monitoring of the civilian population was extensive throughout the Cold War, the subsequent digitalisation of networks, the rise in use of the internet, and prevalence of mobile phones, brought new sources of data, and techniques for state internal security agencies conducting electronic surveillance.[22] Simultaneously, the emergence of transnational non-state actors as a national security priority, particularly in the US – the largest provider of security assistance - has been reflected by changes in security assistance policy and funding.[23]

What it Looks Like Now: Law Enforcement and Military Security Assistance

United States

In 2001, the US spent $5.7 billion in security aid – in 2017 it spent over $20 billion.[24] In 2015, military and non-military security assistance in the US amounted to an estimated 35% of its entire foreign aid expenditure.[25]

In 2016, the US departments of Defense and State trained approximately 122,500 students from 155 countries, the total cost of which was approximately $953.9 million.[26] Activities financed include programmes focusing on counter-narcotics and counter-terrorism issues, the training and equipping of militaries in African countries for crisis response and peacekeeping purposes, and the financing of a range of affiliated worldwide centres and fellowships.

Department of State

Examples of US providers of security assistance include the State Department’s Bureau of International Narcotics and Law Enforcement Affairs (INL), which since 1995 has funded and administered International Law Enforcement Academies (ILEA) aimed at “advanc[ing] the anti-crime effort through building the capacity of foreign criminal justice partners of the United States” and “expanding the skills of partner-nation law enforcement affairs, fostering partnerships across national borders within important regions of the world, and improving partner nations’ relationships with American law enforcement agencies.”[27] Currently, academies led by different US agencies each serve personnel from regional countries:

Hungary	Federal Bureau of Investigations
Thailand	Drug Enforcement Administration
Botswana	Federal Law Enforcement Training Center
Peru	Federal Law Enforcement Training Center
El Salvador	Federal Law Enforcement Training Center
New Mexico	State Department

Training, delivered by personnel from across US government agencies, includes courses on Computer Crime Investigation, Counter-narcotics, and Counter-terrorism. In 2017, the ILEA in Botswana featured courses on Narcotics Investigations delivered by the DEA to over 30 students,[28] on counter-terrorism and cybercrime delivered by the FBI, and on “Investigations of Computers and Electronic Crimes” delivered by the US Secret Service to 30 students from South Africa, Lesotho, Nigeria, Ghana, and Botswana.[29] Training by the DEA includes “the use of tactical and strategic intelligence; coordinated surveillance operations; the safe utilisation and management of informants; the employment and protection of undercover operatives and the planning and execution of tactical operations” as well as training on “interviewing and interrogation”.[30] In total, over 60,000 individuals from 85 countries have graduated from the Academies.[31]

Other US training programmes include the State Department’s Anti-Terrorism Assistance (ATA) Program which has “successfully delivered services” to 100,000+ law enforcement personnel from 154 countries. Between 2012 and 2018, State allocated about $715 million to the program.[32] “Through a blend of training, equipping, mentoring, advising, and consulting partner nations”.[33] For example, between 2008–2013, 17 courses were taught in Morocco under the program to 129 participants from the two leading law enforcement agencies, the Royal Gendarmerie (*Gendarmerie Royale*—GR), and the General Directorate for National Security (*Direction Générale de la Sûreté Nationale*—DGSN), of which 11 courses were on “Cyber Forensics”.[34] According to an assessment, the program “has doubled [the DGSN’s] rate of organizational growth for cyber-investigative capacity” and allowed the Gendarmerie Royale to combine “enhanced cyber-forensic capabilities with database analysis to develop a new approach that they credit with producing a downturn in criminal activity”.

Under the ATA program in 2009, a central monitoring facility was established in Jordan, which includes a “geographic information system (GIS) covering 568,000 landmarks throughout Amman, a city-wide closed circuit TV (CCTV) network, an Automated Number Plate Recognition (ANPR) system to read license plates captured in CCTVs, a Mobile Video Recorder System, and an Automated Vehicle Locator (AVL) to track the location of police vehicles.”[35]

The US State Department has also financed and granted a range of surveillance equipment to foreign countries, including:



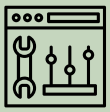
The financing of a monitoring centre designed to ‘intercept, analyze and use intercepted information from all types of communications systems operating in Mexico’, and deployed by US/Israeli surveillance company, Verint.[36]



13 ‘communcations intercept sets’ which were donated to the Venezuelan National Drug Office[37]



The donation of a range of computer forensic equipment and 113 units of ‘specialized surveillance equipment’ to the Surveillance Unit within the Service for Combating Organized Crime in Serbia[38]



The funding of a wiretapping system and assistance in collection of evidence in Uruguay, without which “many anti-narcotics projects would not be possible in their current form”.[39]



The donation of ‘electronic surveillance equipment and tools’ to the Bahamas Drug Enforcement Unit and funding of its subsequence maintenance, as well as the training on the use of the equipment for Bahamas officers in the United States.[40]



The provision of biometric traveller screening systems developed by defense contractor Booz Allen Hamilton – the Personal Identification Secure Comparison and Evaluation System - to Burkina Faso, Cameroon, Chad, Djibouti, Ethiopia, Kenya, Mali, Niger, Tanzania, Uganda, Iraq, Jordan, Yemen, Maldives, Afghanistan, and Macedonia.[41]



The funding of a 2016 project to “support the development of a Fusion Center for Argentine security forces, based on the US model, to expand capabilities and improve communications and information sharing between Argentine federal ministries” and “hosted Argentine counterparts and organized training courses in counterterrorism and fusion center strategic planning”.[42]

An analysis of data contained within the 6,000 Department of State diplomatic cables undertaken by the Intercept in 2016 found that training was being conducted in ‘no fewer than 471 locations in 120 countries — on every continent but Antarctica — involving, on the US side, 150 defense agencies, civilian agencies, armed forces colleges, defense training centers, military units, private companies, and NGOs, as well as the National Guard forces of five states.’[43] Rachel Kleinfeld, a senior associate at the Carnegie Endowment for International Peace and former member of the State Department’s Foreign Affairs Policy Board, is quoted as saying that “There are more than 180 authorities and scores of agencies working in these areas, and the way it has evolved over time has made it absolutely impossible for anyone to know what’s going on. ... There really is no oversight”.[44]

Department of Defense

Prior to 9/11, the US government was funding 57 security assistance programs; by 2017, it was funding 102, according to WOLA’s “Global Guide.”[45] Of the 50 new programs added since 2001, 48 were funded by the US Department of Defense, “with the bulk focused on counterterrorism. Through these 107 programs, the United States funds well over $20 billion in activities, equipment and services in over 160 countries.”[46] According to WOLA, the top six programs provide military equipment; support for Afghanistan’s military and security forces; global anti-drug programs; counterterrorism capacity in Africa and the Middle East; counterterrorism capacity in Iraq, Afghanistan and Syria; and support to Iraq against the Islamic State.[47]

Africa is a key focus of US government-funded military and security training. This was underlined in a “posture statement” in March 2018, from AFRICOM to two US House and Senate committees by US Marine Corps Gen. Thomas D. Waldhauser, the commander of AFRICOM.[48] “On any given day,” the general said, “up to 7,200 US uniformed personnel, Department of Defense civilians, and contractors are in Africa,” while security operations “are executed almost exclusively by the partnered security forces.” To ensure proper oversight, Gen. Waldhauser said AFRICOM works in concert with the Department of State and other agencies “to develop human rights-respecting security forces and inspire them to pursue military professionalism in their institutions.” AFRICOM, the general said, utilises specific skills provided by the State Department, USAID, the FBI, DHS and DOJ, with many of these agencies having a “liaison cell” within AFRICOM to “synchronize and complement our approach.” The statement included details about many of AFRICOM’s training and partnership programs:



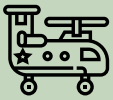
Reconnaissance and surveillance capabilities for counterterrorism operations are in place in East Africa, including Unmanned Aerial Vehicles (UAV) deployed by Kenya and Uganda against al-Shabaab in southern Somalia.



In Tunisia, US forces train and equip the country’s special operations forces and provide mobile ground surveillance radar and ISR aircraft to monitor the border with Libya.



In Niger, AFRICOM provides training and equipment to the Nigerien Armed Forces and counterterrorism advice to Nigerien combat units.



In Burkina Faso, US forces support “intra-theater mobility operations” and provide training to counterterrorism operations.



In Chad, US forces conduct security force assistance with the Chadian Special Anti- Terrorism Group.



Working with the State Department and other agencies, AFRICOM’s Security Governance Initiative “builds the capacity of civil and defense institutions” in Ghana, Kenya, Mali, Niger, Nigeria and Tunisia.



Benin, Cameroon, Chad, Niger and Nigeria are joined in a Multinational Joint Task Force that coordinates operations and intelligence-sharing with US forces.



In its testimony, AFRICOM disclosed problems in only one country, Nigeria. There, the US is expanding intelligence-sharing agreements and cooperation despite partners in the Multinational Joint Task Force who “sometimes fall short of respecting international norms of human rights when dealing with local populations.” Specifically, they have used “heavy-handed counter-insurgency techniques” that have led to civilian displacement and forcible returns of Nigerian refugees from neighboring countries; these practices “produce the grievances that fuel support for the enemy,” AFRICOM admits.

The massive US base at Camp Lemonnier in Djibouti serves as the “vital hub” for US security assistance, operations and logistics for AFRICOM, three other combatant commands and the US Special Operations Command. The US presence at Camp Lemonnier is so large that the $200 million in contracts awarded to local vendors represents nearly 14 percent of the total gross domestic product of Djibouti, according to an AFRICOM press release.[49]

The US Department of Defense also provides various other forms of security assistance through a myriad of programmes. One such programme is the Counterterrorism Partnership Fund, which aims to “support a transition to a more sustainable and partnership-focused approach to counterterrorism” by “build[ing] on existing tools and authorities to respond to a range of terrorist threats by providing direct support to partner nations as well as augmenting US capability to support partners in counterterrorism (CT) operations”.[50] Proposed by President Obama in 2014, the Department of Defense requested $2.1 billion for the fund for FY 2016.[51] In addition to training and equipping various border security forces around the world funding intelligence fusion centers, the request includes allocations for:

...“the purchase of US equipment to support Intel sharing”, developing “coordinated intelligence sharing with appropriate African [counterterrorism] partners” and providing “near-real-time mutual sharing of technical classified intelligence between the US and Kenya to enhance [counterterrorism] operations.”

...enhancing “the capability of Maghreb and Sahel [counter terrorism] forces to collect, analyze, and disseminate intelligence … and training and equipping for command and control nodes, fusion centers, and military intelligence units.”

...“enabling US military units under Africa Command to support partners with “targeting, intel planning, collection management, intelligence and warning, operational analysis, and intel for named operations and partner nation capacity building activities.”

...allowing West African nations to “gather, analyze, and disseminate intelligence” related to Boko Haram.

...building “bilateral networks that enable the US to securely share timely, relevant intelligence with partners”.

...providing “critical counterintelligence (CI) and human intelligence (HUMINT) mission management technologies to enhance partner nation information sharing”.

Since 2002, the US has appropriated $76 billion for various Defense and State programs aimed at supporting security in Afghanistan.[52] The US also provided the Afghan Automated Biometrics Information System, including fingerprint, palm, and iris scanners used to collect personal identification information, as well as the Afghan National Tracking System, a system composed of various items including global positioning system equipment used to provide location and identification data of Afghan forces. Between 2006 and 2017, the Department of Defense provided 120 radio monitoring systems, 22 ground-based operational surveillance systems, 8 unmanned air systems, and 6 surveillance balloons to the Afghan National Defense and Security Forces.[53] The Afghan Ministry of Interior is currently developing a lawful intercept program – used for wiretapping telecommunications networks – with the aid of a working group comprised of Coalition and Afghan members.[54]

Department of Justice

The US Department of Justice also carries out its own foreign assistance under the International Criminal Investigative Training Assistance Program (ICITAP), with funding from State, Defense, and Agency for International Development. The program currently funds projects in 35 countries,[55] and has trained over 17,000 individuals in FY 2017 on topics including Terrorism and Transnational Crime, Cyber Crime, Forensics, “Specialized and Tactical Skills”, and Border Security.[56] For example, under the Program, ICITAP set up a biometric screening system in Bosnia-Herzegovina,[57] as well as a computerised database and software border control network. The network, developed and donated by ICITAP for use by border police, connects the country’s border crossings, including four airports, with the Directorate for the Police Body Coordination (DCPB), the State Investigative and Protection Agency (SIPA), the Federation Ministry of Interior, and the BiH Ministry of Security, and allows access to other databases, including those of INTERPOL.[58]

Schools of Surveillance

The US government is training hundreds of foreign military officers in the techniques of military intelligence and surveillance/signals intelligence in two of the Pentagon’s most important intelligence facilities, as well as a school run by the Defense Intelligence Agency, according to Pentagon and State Department reports submitted to Congress.

The two facilities are Fort Huachuca in Arizona, the home of the US Army Intelligence Center, the premiere center for the training of US military interrogators; and Fort Gordon in Georgia, the site for one of the National Security Agency’s largest listening posts in the world. Both schools rely heavily on private contractors to perform the training. The DIA training is run by the National Intelligence University.

Fort Huachuca

In 2006 and 2007, the US Army Intelligence Center at Fort Huachuca in Sierra Vista, Arizona, sponsored 195 classes for foreign military officers.[59] This training facility came under sharp focus during the Iraq War after eight US Army officers investigated for abuse at the Iraqi prison at Abu Ghraib were stationed there prior to their deployment to Iraq.[60] After the abuse became a national scandal, such training greatly expanded.

In 2006, the *Washington Post* reported, “the greatest one-year expansion of the Army’s interrogation program, from 500 to 1,000 trainees, which took place in 2005, the year after public disclosure of the scandals…Today, with the Army introducing a new interrogation manual and Congress wrestling with legislation sought by the White House that would legalise the CIA’s more aggressive questioning techniques, the number of people training to be interrogators is to rise again.”[61] At the time, the Post reported, subjects covered by the contracted training included “how to interrogate and debrief enemy personnel, potential threat forces, warrior skills, intelligence analysis, and military justice and intelligence law.”

Countries with personnel currently trained at Fort Huachuca include Botswana, Cameroon, Djibouti, Gambia, Kenya, Liberia, Niger, Nigeria, Sierra Leone, South Korea, the Philippines, Bosnia-Herzegovina, Georgia, Kosovo, Serbia, Algeria, Egypt, Jordan, Kuwait, Morocco, Oman, Saudi Arabia (which appears to have the largest number of students), Tunisia, Pakistan, Barbados, Belize, El Salvador, and Suriname.[62]

Fort Gordon

In 2006 and 2007, the Signals School at Fort Gordon sponsored 113 classes for foreign military officers.[63] Classes at Fort Gordon, which defines itself as the “Home of the US Army Cyber Center of Excellence,” include training for “Signal Basic Officers” and “Information Systems Management.” Countries that sent personnel there for training include Burkina Faso, Djibouti, Kenya, Malawi, Swaziland, South Korea, Georgia, Kosovo, Moldova, Montenegro, Ukraine, Bahrain, Egypt, Jordan, Kuwait, Lebanon, Oman, Tunisia, Bangladesh, Krygyztan, and Maldives.[64]

The school is run by Fort Gordon’s Signal Center of Excellence (SIGCEN), which “trains, educates, and develops adaptive Leaders and IT professionals” and also “synchronizes, experiments, and implements Future Network capabilities,” a reference to the NSA’s role as a provider of operational security to military and intelligence communications organizations.[65]

Use of Contractors

Many of the US-funded courses in military intelligence, signals intelligence, ISR, Special Operations and policing/security are run by private contractors. They range from small, focused companies to large, well-known military contractors. Some programs, such as the DOJ’s International Criminal Investigative Training Assistance Program, are run almost entirely by contractors.

Historically, one of the consequences of the vast privatisation of US security and military forces over the past 20 years has been an inappropriate influence of contractors on policy. This is particularly true in the outsourcing of security and military training in Iraq and Afghanistan. According to a 2011 joint audit conducted by the Inspector Generals of the Pentagon and Department of State of police training in Afghanistan:

> “DoD and DOS officials did not develop a comprehensive plan or develop a memorandum of agreement to guide, monitor, and assign transition responsibilities. Instead, officials relied on independently developed contractor plans, some of which were not feasible and did not address inherently governmental tasks. This occurred because DoD and DOS lacked guidance for planning a transition of contract administration responsibilities from one agency to another, which contributed to contractor schedule delays. In addition, DoD officials reported that the incoming contractor did not have 428 of the 728 required personnel in place within the 120-day transition period, which placed the overall mission at risk by not providing the mentoring essential for developing the Afghan Government and Police Force.”[66]

Seven years later, the over-dependence on contractors has not changed. A Defense Department Inspector General report published in January 2018 concluded “that the Afghan air force was too dependent on foreign contractors, noting that contractors were responsible for 80 percent of all maintenance work, while Afghans conducted just 20 percent.” According to the OIG report, the contracts “limit the progressive transfer of maintenance responsibilities to Afghan air force maintainers” and did not include “timelines for transitioning maintenance work to local forces.”

The following contractors are prominently mentioned throughout US government reports on overseas security training:

DynCorp International

is the largest US contractor in Afghanistan and is deeply involved in US security and counterinsurgency (also known as “contingency”) operations around the world as a provider of logistics, aviation and military and intelligence training. A DynCorp pamphlet obtained at a 2017 Washington exhibition of the Association of the US Army explains that much of its training is focused on aircrews and maintenance. “Our global program support encompasses all branches of the US Armed Forces and the US Department of State. We also support national, state, and local governments with expert training.” DynCorp’s training, according to this pamphlet, includes “education, training and certifications for police, intelligence officials, and mission-support operational personnel.” Until 2018, it held the Worldwide Aviation Support Services (WASS) contract with the State Department’s Bureau of International Narcotics and Law Enforcement Affairs.

Leidos Inc.

is one of a handful of companies that dominate privatised intelligence in the United States. As was reported in The Nation, it was formed in 2016, when Leidos Holdings, a major contractor for the Pentagon and the NSA, completed a long-planned merger with the Information Systems and Global Solutions division of Lockheed Martin, the global military giant. The 8,000 operatives employed by the new company do everything from analysing signals for the NSA to tracking down suspected enemy fighters for US Special Forces in the Middle East and Africa. As the Leidos web page on training states, the company will “develop, deliver, and maintain holistic live, virtual, and constructive (LVC) training systems to support force protection for fixed, semi-fixed, and expeditionary sites resulting in improved information management, operational performance, and efficiency.” One of its largest contracts, described below, is providing training at the US Army intelligence school in Fort Huachuca, Arizona.

AAR

describes itself as “an independent provider of aviation services to commercial and government customers in more than 100 countries.” It is a large, highly profitable company that, among other things, is tasked by the US government to fly diplomats around the world. It competes intensely with DynCorp. It currently holds the Worldwide Aviation Support Services (WASS) contract with the State Department’s Bureau of International Narcotics and Law Enforcement Affairs, which provides education and training to foreign police and intelligence officials. AAR is deeply involved in covert operations as a contractor; in 2018 it signed a logistics contract with the US Naval Special Warfare Group also known as SEAL Team 6, the team that assassinated Osama bin Laden.[67] AAR has also been the subject of several investigations; in 2017, it was banned by the US military from using a key airfield in Afghanistan because of safety violations. [68]

North American Surveillance Systems (NASS)

provides training in ISR techniques critical to wars against terrorist groups in Chad, Niger and other countries where AFRICOM has a large presence. It is one of the only contractors listed as a trainer in the bi-annual Pentagon and State Department reports to Congress on overseas training. NASS’s primary business is modifying aircraft so they become “sophisticated solutions for Intelligence, Surveillance and Reconnaissance (ISR) system for domestic and foreign militaries as well as law enforcement agencies and “private special mission companies,” according to its website.

PAE Government Services PAE

(Pacific Architects and Engineers) “supports the implementation of US foreign policy objectives through worldwide diplomacy missions,” its website states. It has major training contracts with the US government in Afghanistan, including a $59.9 million contract signed in December 2017 with the State Department’s Bureau of International Narcotics and Law Enforcement Affairs.[69] One of its largest contracts is a $142 million project with the US Army to “provide logistics support, training and mentoring” to Afghanistan’s National Defense and Security Forces.[70] In 2017, it reached a $5 million settlement with the US government after a whistleblower accused the company of failing to conduct background checks on hundreds of employees on its civilian police contract in Afghanistan, Haiti, Lebanon, Liberia, South Sudan, and elsewhere.

Engility

is a well-connected company with decades of experience in classified US intelligence operations. It runs training programs provided by the Department of Justice’s International Criminal Investigative Training Assistance Program in the Balkans, Mexico and Ukraine. According to the company’s website, its contracts with ICITAP include “program implementation methods focused on being executed on-the-ground in the host country” as well as “pre-program assessments; program planning, program management & review.” Engility support also includes: “curriculum development; classroom training, seminars and workshops; internships; equipment donations; donor coordination; and on-the-job training and mentoring by our embedded long-term advisors.”

Obera LLC

a Virginia company involved extensively with AFRICOM. “Throughout the past three years,” its website states, “Obera has conducted ‘Engagement in Depth’ throughout Africa and other Combatant Commands Area of Operations in support of various US, United Nations and NGO programs. As a Prime Contractor under the Counter Narcotics and Global Threat (CN&GT) Operations and Logistics Support multiple-award IDIQ contract, we remain well positioned to build on our past performance in Africa.” Obera has undertaken US government-financed training in Nigeria, Niger, Chad, Mali, Ghana, Togo, Benin, Burkina Faso, Ethiopia, and the African Union.

Contractors at Fort Huachhuca & Fort Gordon

The prime contractor for training programs at Fort Huachuca is Leidos Inc., one of the nation’s largest intelligence contractors.

Leidos provides its services under the Fort Huachuca Training and Support Contract (HTASC), with a focus in “the areas of instruction and training, training development, training support” and other IT and related services, according to a copy of the contract published on line by Leidos. Disciplines covered include all the basics of military intelligence, including all-source, imagery, signals intelligence, counterintelligence and human intelligence. Some of the training is conducted abroad: contractors “may be required to travel to various locations within the continental United States (CONUS) and outside CONUS (OCONUS).[71]

As the prime contractor, Leidos hires subcontractors for these positions, plus other contractors may be involved in work separately. Companies hiring for training positions at Fort Huachuca, according to the contract job site Indeed.com, include Calibre Systems Inc., General Dynamics Information Technology, Northrop Grumman, Trace Systems, Raytheon and Jacobs.

RLM Communications Inc, one of the instruction contractors at Fort Gordon, claims that the outsourcing of operations at Fort Gordon began in earnest during the Bush administration.

> “Based upon an analysis of contracting requirements since the commencement of the Global War on Terrorism (GWOT) in 2003, the SIGCEN has determined that a significant quantity of these are recurring, short-notice actions that could be more rapidly and efficiently met with a multiple-award, task order driven, Indefinite Delivery / Indefinite Quantity (ID/IQ) contract to meet projected requirements.”[72]

Contractors are deeply involved in the development of the curriculum at Fort Gordon. A solicitation for business from the US Army and Fort Gordon posted on *FedBizOps* in March 2018 for “training for 24 students” states that “the United States Army Cyber Center of Excellence requires contractor support for Signal Technician Training and Support courseware development and instruction for the Network Management Division at the Leader Network Operations College, Signal School, Fort Gordon, GA.”

Contracted instructors at Fort Gordon also have access to classified intelligence: “All contractors”, the solicitation states, “shall have a SECRET security clearance and shall maintain the required security clearance throughout the life of the contract. The contractor is responsible for acquiring the clearances.” Some of the contracted trainers must also have clearances high enough to access SIPRNET.

This highly classified gateway network, according to the Defense Information Service Agency (DISA), “provides DoD customers with centralized and protected connectivity to federal, Intelligence Community (IC) and allied information at the secret level.”

The trainers, RLM Communications claims, are involved in every aspect of the school, including “course development and instructor services, course analysis, design, development and specific classroom instruction.”

In addition to RLM, ManTech International, a large US intelligence contractor, holds a contract for a “master trainer” at Fort Gordon “to effectively direct the organization’s education, training and development programs to successfully meet the customer’s organizational goals.” According to the ManTech website, it is also hiring for a “Regional Operations Manager” in Fort Gordon to “oversee and manage operations in support of the training on new and existing C4ISR Technology and any emerging Cyber technology,” ManTech also provides training for military forces in Egypt and Saudi Arabia.

US-Funded Training in Intelligence, Surveillance and Reconnaissance (ISR)

As US military strategy and spending has focused increasingly on nations facing internal insurgencies and threats from ISIS and other terrorist organisations, the US military, particularly the US Air Force, has turned much of its attention on building and expanding its ISR capabilities around the world.

“The evolution of globally integrated ISR has fundamentally changed how America fights wars,” the US Air Force declared in ‘Air Force ISR 2023’,” a “strategic vision” paper prepared for the Pentagon during the Obama administration. “It is the foundation upon which every joint, interagency, and coalition operation achieves success.”

ISR operations involve spy planes and drones equipped with sensors and other surveillance equipment, used to fly over countries such as Afghanistan and Libya to find and track terrorist groups. The lethal nature of these aircraft and their tracking abilities were recently described in The Drive, a US publication about military technology, in an article about two new planes called “Dash-8s” the US Special Operations Command (SOCOM) recently deployed in Libya to kill ISIS militants:

> With this equipment on board, both types of planes had the mission of performing persistent surveillance missions across relatively wide areas, using their sensors to build larger maps of entire regions. From there, analysts could examine the imagery for items of interest, potentially establishing so-called ‘patterns of life’ for specific terrorists or small groups of militants.

The Army primarily employed them to hunt for improvised explosive devices and, by extension, to trace insurgent movements back to bomb workshops or other base camps. That same wide-area surveillance information can help US forces determine when the best opportunity might be to try and kill or capture a particular individual with as little risk to nearby innocent civilians as possible.

The importance of ISR to US-backed counterinsurgency operations can be seen from the example of Nigeria, which has received extensive support from the US government, including the shipments of surveillance aircraft. In December 2017, the US ambassador to Nigeria presented the country with 12 A-29 “Super Tucano” surveillance aircraft to the Nigerian Air Force. The planes were delivered in the midst of a series of operations launched by Nigerian security forces against Boko Haram terrorists. “The operations started with an (ISR) mission,” DefenceWeb reported. It added that the $593 million deal with the US government will “permit sustained and effective round the clock COIN [counterinsurgency] operations” by the Nigerian Air Force. “The mission can be effective only when it is supported by adequate ISR…NAF is presently not very well equipped in this regard.”

With the expansion of US operations in Africa, ISR spending has become a major thrust for AFRICOM and its training programs. AFRICOM’s 2018 Posture Statement, presented to the US Congress in March 2018, states that the 2019 budget for Africa “includes appropriate resources — notably, Intelligence, Surveillance, and Reconnaissance (ISR) assets.”

US government training in ISR is focused heavily on Africa and Central and South America. Much of the training is conducted by contractors, led by North American Surveillance Systems (NASS), Ansible Government Solutions, Orbital ATK, and General Dynamics. According to the US government’s 2016-2017 “Foreign Military Training Report,” ISR training is taking place in:

- Chad – provided directly by NASS.
- Niger – provided directly by NASS
- Mauritia – ISR Flight and Ground Training provided in-country
- Tunisia – ISR flying training provided in-country (likely to expand significantly after US DoD notified Congress in March 2018 of its intention to provide an additional $20 million worth of sensors “to help Tunisia secure its border security wall that separates it from Libya.[73] ”)
- Philippines – provided directly by NASS

For US allies in Central and South America, ISR training is provided at Inter-American Air Forces Academy (IAFFA) in Lackland, Texas, for personnel from Argentina, Colombia, Honduras, Mexico, Panama and Peru.

The IAFFA courses in ISR are available online. One class “is designed for officers, enlisted, National Police and civilian equivalent requiring an understanding of the fundamentals of Intelligence, Surveillance, and Reconnaissance. Graduates will learn basic principles of intelligence, analysis, critical thinking, Intelligence Preparation of the Operational Environment (IPOE), ISR concepts and roles, and targeting fundamentals. They will receive training in plotting coordinate systems and presenting intelligence briefings.”

In another recent deal that underscores the importance of ISR to African nations, the US State Department donated several unmanned aerial vehicles to the African Union Mission (Amisom) in Somalia “to provide enhanced ISR capability.” According to the African military publication DefenceWeb, the UAVs “appear to be Aerostars manufactured by Israel’s Aeronautics Defence Systems but possibly acquired through General Dynamics in the United States.” General Dynamics, a major US military contractor, has had a strategic alliance in place with Aeronautics since 2004, under which the Israeli company provides UAVs to the “US market and select international customers”.

Europe

Security assistance is provided under the auspices of the European Union (EU) to EU and non-EU countries, as well as by individual EU member states. Spending on such assistance is set to rocket in Europe as a result of the European Union proposing to increase such expenditure and projects.

European Union

EU funds have been provided to member states to conduct mass surveillance. For example, €25 million from the European Regional Development Fund’s (ERDF) was allocated to Romania’s intelligence agency to boost their technical ability to intercept communications, conduct facial recognition, and giving them aggregated access to databases owned by public institutions, including a database of 50-60 million peoples’ images.[74] In 2013, €50 million from the Prevention of and Fight Against Crime budget was made available to set up national Passenger Name Records (PNR) systems, in effect establishing the infrastructure for a mass travel surveillance system before any EU legislation was in place.[75]

Various EU agencies and instruments currently finance or train security agencies in third countries within the Commission, as part of the Common Security and Defence Policy, and as part of the Common Foreign and Security Policy. Established in 2014, the Instrument Contributing to Stability and Peace (IcSP) is one of the main external assistance mechanisms, focusing on delivering short-term assistance aimed at crisis response, conflict prevention and peace-building. The IcSP has a budget of €2.3 billion for 2014-2020 and currently funds 288 projects in 71 countries.[76] Current projects include developing the capacity of Tunisian security agencies to counter terrorism by developing “intelligence processing and analysis”, “providing training in digital intelligence gathering including through social media and digital mapping”, and “developing inter-service cooperation among Tunisian security agencies”. Other projects aim to develop the internal security service in Burkina Faso by improving “Intelligence cycle management”, support “the planning and gathering, as well as the coordination, of intelligence efforts” in Somalia, and establish a counter-terror information coordination centre with the Iraqi National Security Council aiming “to foster coordination and ensure that the seven Iraqi intelligence services work together effectively.”[78]

The African Peace Facility, which has received €2.1 billion from the European Development Fund (EDF), finances peacekeeping and early response capabilities in African countries as well as capacity building for security institutions, including the operationalisation of the African Union’s African Peace Security Architecture (APSA).[79] APSA’s 2016-2020 roadmap, developed by the AU, includes as a priority the training and support of law enforcement agencies to counter terrorism, including through “information and intelligence gathering and analysis”, “investigations and evidence gathering” challenging “internet abuse”, and the development of “platforms for intelligence sharing and coordination”.[80]

Reacting to wide press coverage of the ’migrant crisis’, the EU launched the Emergency Trust Fund for Africa in 2015, aiming to tackle irregular migration by, amongst other things, “enforcing the rule of law through capacity building in support of security and development as well as law enforcement, including border management and migration-related aspects” and contributing to “preventing and countering radicalisation and extremism.”[81] The fund, with a budget of 3.2 billion euros, has 117 programmes across the three regions as of November 2017.

Under the fund, the European Commission allocated €40 million to Sudan in 2016 for border management and capacity building for the judiciary and law enforcement. A EU risk analysis document leaked to the media identified the “provision of equipment and trainings to sensitive national authorities (such as security services or border management) diverted for repressive aims; criticism by NGOs and civil society for engaging with repressive governments on migration (particularly in Eritrea and Sudan)” as a risk of the programme.[82] EU funding for border management in Sudan has included the funding of units in which personnel are former members of the Janjaweed militia, responsible for atrocities during the Darfur genocide.[83]

Frontex, the EU’s external borders agency, has concluded working arrangements with authorities in 17 countries, which include financing and training activities,[84] and maintains information sharing mechanisms with regional countries within Africa-Frontex Intelligence Community (AFIC), the Western Balkans Risk Analysis Network (WB-RAN) and the Eastern Risk Analysis Network (EaP-RAN). Frontex has allowed Libyan Coast Guard “with limited access to Frontex Fusion Service” and provided training on its use, and has trained Libyan Coast Guard officers on “Law Enforcement at sea”.[85]

In May 2018, the European Union unveiled proposals that will see substantial increases on security assistance programmes as part of the Multiannual Financial Framework (MFF), which determines the EU’s expenditure between 2021-2027:

€13 bn
2014-2020

€33 bn
2021-2027

For example, the EU budget for the management of external borders, migration and asylum is proposed to triple from the previous budget, to reach around €33 billion, compared to €13 billion for the period 2014-2020.

€95 bn
2014-2020

€120 bn
2021-2027

Funding for external action is proposed to increase by 26% from the previous budget, to reach €120 billion, with a specific emphasis dealing “with emerging challenges, notably in the area of stability and migration”, according to the European Commission.[86]

€3.5 bn
2014-2020

€4.8 bn
2021-2027

€13 bn
PROPOSED

Expenditure on security is proposed to increase by 40% to reach €4.8 billion, while a new Defence Fund worth €13 billion is proposed to be set up, which will be provided to arms companies and researchers to catalyse research and development in security and defence technology.

Diversion of Development Funds

The security-focused policy of the EU has led to a diversion of money for development towards security projects. Initial recognition of a ‘security-development nexus’ by EU institutions in 2006 outlined in the European Consensus on Development began efforts to use security assistance to meet development objectives.[87] Such moves have resulted in, for example, a July 2016 proposal seeking to alter the Instrument Contributing to Stability and Peace, which is currently used to provide security assistance to civilian agencies, to also train, finance, and equip military actors in third countries.[88] In December 2017, amendments were added allowing the Instrument to be used for “the provision of capacity building programmes in support of development and security for development, including training, mentoring and advice, as well as the provision of equipment, infrastructure improvements and services directly related to that assistance”. Under the regulation, €100 million will be available for capacity building programmes of military actors in non-EU countries.[89]

It further resulted in 97% of the budget allocated to migration management funding migration containment, instead of projects “that enhance migration’s positive contribution to development and ensuring migration is safer and more orderly”.

According to research by Oxfam 22% of the budget for the first two years of the overall EU Emergency Trust Fund for Africa (of which 80% comes from development and humanitarian aid funds) was allocated to projects in the field of migration management.[90] Another 13.5% goes to peace-building and security, with the largest part (between €121 million and €161 million, or 7% of the total budget) used to fund security forces in third countries, which are implemented by private and public companies.

Oxfam’s research into the fund also revealed that the instrument’s securitised approach resulted in insufficient safeguards, decisions taken without consultation, and insufficient attention to conflict-sensitive measures and ‘do no harm’ principles. It further resulted in 97% of the budget allocated to migration management funding migration containment, instead of projects “that enhance migration’s positive contribution to development and ensuring migration is safer and more orderly”.

European Countries

In addition to the EU bodies, security assistance is also provided by individual EU member states. A range of UK organisations currently fund or train foreign security actors under various funding instruments.

In response to a Parliamentary question regarding Nigeria, Tobias Ellwood, Under Secretary of State at the Foreign and Commonwealth Office, stated that the UK government has provided “a substantial package of military, intelligence and development support including training and advice for the Nigerian armed forces” including the training of over 22,500 Nigerian military personnel and the support of “a Nigerian intelligence analysis and planning cell focused on the North East and based in Abuja”, the provision of £5 million to support a regional taskforce against Boko Haram, and the deployment of UK surveillance aircraft in 2014.[91]

Under the UK’s Conflict, Stability and Security Fund, in 2016-2017 Ukraine’s national corruption body received over £500,000 to establish a digital forensics laboratory and associated training, as well a new database system allowing it to “collect, manage and analyse bulk data more effectively in support of investigations.”[92] The Fund also committed £180,000 to help fund the training of 180 “Cyber Police Officers” and provide “specialised equipment to enable trained Cyber Police officers apply their knowledge in daily work and to establish a cybercrime laboratory.”[93]

UK police provided training in “community policing” techniques in Sri Lanka beginning in 2007, despite government concerns regarding “a veneer of community based policing being used to cover less palatable behaviour”.[94]

In 2016, the BBC reported that the UK College of Policing has provided training to the Saudi Ministry of the Interior in investigative techniques since 2009, and is planning to expand training to include ‘High Tech Crime and IT Digital Forensics training’, ‘I-Phone and GSM mobile telephone GSM examination and analysis’, and ‘Senior Investigating Officer Training’. The strategic objectives for UK Foreign Policy are identified as related to diplomatic, national security, and development objectives:

> “UK / KSA [Kingdom of Saudi Arabia] interoperability is becoming of even greater importance, with the in-country Counter Terrorism and Extremism Liaison Officer now handling evidential as well as intelligence requests, for example the find of the printer cartridge bomb at East Midlands airport in 2010. Therefore any assistance that College can provide to assist developing the evidential gathering and investigative capability and crime scene management of the Saudi Arabia Police could potentially be of benefit for prosecutions in the UK or for prosecutions in the KSA that concern UK interest”.[95]

A UK Parliamentary Home Affairs Committee report published in 2016 concluded that ‘There must be more transparency in the process and Parliament must not be denied the opportunity for proper scrutiny’[96] of the nearly 60 countries with which the College has worked.[97]

The German Federal Criminal Police Office (Bundeskriminalamt) is reported to have provided training to Egyptian authorities on investigating internet users in 2011, weeks before President Hosni Mubarak was forced out of office during the Arab Spring.[98] In response to public pressure and parliamentary questions regarding police training and equipment aid provided to Egyptian security agencies, the government refused to cease or amend the programmes because there had been ‘no information to suggest that in the years 2015 and 2016, knowledge shared with or technology made available to Egypt as part of the training and equipment aid was used improperly or in contravention of constitutional standards.’[99] In October 2017, it was reported that the German government cancelled a workshop aimed at training Egyptian security forces in internet surveillance and identifying sites that “are misused by terrorists to disseminate their extremist ideology and prepare terrorist attacks” because, according to the Federal Foreign Office, “some of the knowledge and skills imparted during this training course could potentially be used not only to pursue terrorists but also to persecute other groups of people”.[100]

A UK Parliamentary Home Affairs Committee report published in 2016 concluded that ‘There must be more transparency in the process and Parliament must not be denied the opportunity for proper scrutiny’ of the nearly 60 countries with which the College has worked.

France has 17 police and military training centres (Les Ecoles Nationales à Vocation Régionale) in 10 African countries. Internal security training, focusing on policing, is provided to officers from 23 countries with a Francophone majority.[101] Created in 2001, Civipol is a large security consulting and training enterprise 40% owned by the French state which currently implements security projects abroad for the French Ministry of Interior. Among other courses, Civipol offers training in investigative techniques, information sharing and gathering, cybercrime, GPS data analysis, and mobile phone location tracing/identification. At present, it is the fourth largest recipient of funds under the EU’s Trust Fund for Africa, and has 40 projects outside of the EU, of which 35 are in Africa.[102] Civipol is an implementing partner of the creation and training of a border force in Sudan.

China

China’s government uses a combination of human and highly advanced technological systems of surveillance to practice political control. As well as targeting religious, pro-separatist, and democratic movements, Chinese security agencies employ highly intrusive surveillance against religious minorities, particularly in Xinjiang, where the Uighur minority are subjected to a wide array of surveillance measures, including by a massive human security presence, the development of a DNA database, iris and body scanners at checkpoints, public facial recognition checks, drones fitted with cameras, and apps which monitor smartphones which are made mandatory.[103] The development of a domestic surveillance industry and capabilities means that Chinese companies and authorities are also exporting surveillance around the world.

In 2015, Chinese President Xi Jinping pledged to continue “to supply Afghanistan with security supplies, technology, equipment, and training assistance.” China has concerns about separatist movements in Xinjiang, which shares a narrow border with Afghanistan.[104] In 2015, Tanzania became a pilot country for China–Africa capacity-building, through which China has reportedly provided technical assistance to influence a Tanzanian cyber-crime law and place restrictions on internet content and blogging activity similar to China’s content controls.[105]

China also uses security cooperation alliances to promote surveillance. China was a founding member of the Shanghai Cooperation Organisation (SCO) in 2001, together with Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan, allowing it to exercise its security interests in the region with Russian acquiescence.

Surveillance technologies are being exported from China’s under the Belt and Road Initiative and other efforts to expand in international markets. Chinese companies have reportedly supplied surveillance capabilities to Bolivia, Venezuela, and Ecuador.[106] In Ecuador, China Electronics Corporation supplied a network of cameras some fitted with facial recognition capabilities to the country’s 24 provinces, as well as a system to locate and identify mobile phones. Chinese companies have reportedly also won contracts for surveillance capabilities in Zimbabwe, Singapore, Malaysia, and Mongolia.[107]

China also uses security cooperation alliances to promote surveillance. China was a founding member of the Shanghai Cooperation Organisation (SCO) in 2001, together with Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan, allowing it to exercise its security interests in the region with Russian acquiescence, including dealing with the threat from alleged Uighur separatist groups and its lingering border disputes in the region. Today its explicit aims are to focus on countering the ‘three evils’ of extremism, separatism, and terrorism in the region. An analysis by the Human Rights Initiative of China reports how the SCO also acts as a platform for intelligence-sharing between members, including through the use of shared databases, and

watchlists. Both Kazakhstan and Uzbekistan have stated in reports to the UN Security Council that they use SCO lists for monitoring, denying entry to, and sharing intelligence on specific individuals.

Pakistan and India both joined the SCO in 2017. The Chinese government has reportedly provided loans to countries in order to facilitate the purchase and use of surveillance capabilities for Chinese providers. Huawei, the international telecommunications company, reportedly installed some 1500 security cameras in Islamabad, Pakistan’s capital, following the provision of a loan between the governments of China and Pakistan in 2010 under Islamabad’s “safe city” project. Dawn reports that the provision of the contract, which was done after waiving the tendering process, was linked to the Chinese government approving the loan. [108]

What We Aren’t Permitted to Know: Intelligence Agencies Assistance

There is extremely limited publicly available information about the extent and application of cooperation among intelligence agencies. The most well-known cooperation agreement, the UKUSA Agreement, began as a series of bilateral cooperation agreements after the Second World War involving the signals intelligence agencies of Australia, Canada, the UK, the US, and New Zealand (known as the Five Eyes). Today, interception, collection, acquisition, analysis, and decryption is conducted by national signals intelligence agencies within their regional areas, with intelligence being shared among other members. The agreement also provides for joint operations as well as staff from multiple agencies working alongside one another.[109] For example, Menwith Hill in the UK has been home to US surveillance equipment and personnel since the 1950s, and is currently being used by the US National Security Agency (NSA) to intercept global satellite and wireless communications, intelligence from which has been used in drone strikes.[110]

Based on documents released by Snowden, it was reported in 2017 that the NSA also provided substantial surveillance capabilities to intelligence units in Ethiopia. In exchange for training and equipment, in 2002 Ethiopian authorities allowed the NSA to set up a signals intelligence operations centre in Ethiopia’s capital, Addis Ababa. By 2005 the centre had grown to include 103 Ethiopian personnel and capacity to monitor communications in Somalia, Sudan, and Yemen, producing “almost 7,700 transcripts and more than 900 reports based on its regional spying effort”.

Cooperation among Western intelligence agencies extends to the ‘Nine Eyes’, which in addition to the Anglophone Five Eyes includes Denmark, France, the Netherlands and Norway; the 14 Eyes, which includes the Nine Eyes, with the addition of Germany, Belgium, Italy, Spain and Sweden (which has access to internet traffic travelling along submarine cables from Russia); and the 41 Eyes: which includes the 14 eyes plus the allied coalition in Afghanistan.

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.”[111] Under RAMPART-A, the codename of a programme revealed by Snowden, foreign partners ‘provide access to [submarine] cables and host US 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, nine of which were active in 2013.[112] 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.[113] In 2014, it was reported that the UK’s main signal intelligence agency, Government Communications Headquarters (GCHQ), had a similar programme in Oman tapping submarine cables.[114]

Based on documents released by Snowden, it was reported in 2017 that the NSA also provided substantial surveillance capabilities to intelligence units in Ethiopia.[115] In exchange for training and equipment, in 2002 Ethiopian authorities allowed the NSA to set up a signals intelligence operations centre in Ethiopia’s capital, Addis Ababa. By 2005 the centre had grown to include 103 Ethiopian personnel and capacity to monitor communications in Somalia, Sudan, and Yemen, producing “almost 7,700 transcripts and more than 900 reports based on its regional spying effort”.

Similarly, in 2017 The Intercept reported that for over six decades the NSA has maintained at least three bases in Japan, which has contributed more than half a billion dollars to finance its facilities and operations, in exchange for surveillance equipment and the sharing of intelligence.[116]

Conclusion – Assisting Human Security

States with large security architectures are instrumental in sponsoring surveillance capabilities around the world through numerous security cooperation agreements, development assistance programmes, security sector reforms, and post-conflict reconstruction programmes. This will remain a priority for them with the lure of intelligence and political influence and the nature of transnational crime. States which export such capabilities have themselves responded to advances in technology by expanding and developing new surveillance powers themselves, but have at the same time failed to develop adequate legislation and safeguards to accompany many of these powers, and various courts have found techniques practiced by security agencies to be unlawful.[117] The export of these surveillance capabilities, sometimes to places which lack basic rule of law, therefore carries significant and foreseeable risks to the security and rights of individuals.

In many cases, such as the support of surveillance and security agencies in authoritarian states, the risk of facilitating human rights abuses is considered an acceptable price to pay for buying other forms of influence.

In many cases, such as the support of surveillance and security agencies in authoritarian states, the risk of facilitating human rights abuses is considered an acceptable price to pay for buying other forms of influence. During the Cold War, the provision of military aid to allied nations or former colonies was considered vital to exerting influence to counter an opposing bloc; today it is transnational issues such as counter-terrorism, trafficking, and migration which are drawing states with large security apparatus to sponsor surveillance worldwide. Authoritarian dictators, such as Sudan’s al-Bashir - the first world leader to ever be indicted by the International Criminal Court for war crimes – are being generously empowered with funds and security capabilities if they promise to keep people from the shores of Europe. The immediate outlook, as demonstrated by the EU’s commitment to dramatically increase spending in these areas, is that the promotion of security and surveillance will take an even higher prevalence over human rights and development – and it will use development money to do so.

The arms industry and contractors, which already benefit substantially from these surveillance programmes – stand to benefit even more, which will only naturally increase their potentially damaging influence over public policy, as exemplified during the most recent invasions of Afghanistan and Iraq by US-led coalition forces.

While much of the situation is the result of calculated policy-making, it is clear that much also results from the inability to efficiently manage and coordinate all such programmes when, as in the US, there are so many different priorities, agencies, and departments involved. This is massively compounded by the fact that secret

intelligence agencies, whose work is largely unknown to separate government agencies or policy-makers, are also involved in providing surveillance capabilities to foreign government agencies, including in authoritarian regimes.

Mitigating this requires fundamental reforms to foreign assistance programmes and how they promote surveillance capabilities. At the most basic level, due diligence – such as efforts to ensure that training is not provided to units or individuals involved in gross violations of human rights, laid out for example in the Leahy Law in the US - are frequently criticised as insufficient.[118] Transparency about the types of assistance being provided, key to ensuring effectiveness and adequate democratic oversight, is uneven and wholly lacking for the intelligence agencies.

Ensuring that it contributes to longer-term security however depends on prioritisation and objectives: securing governing structures, critical infrastructure, or territory, which may provide short-term stability or cooperation, is different from securing individuals, especially in contexts where definitions of national security and terrorism are overly broad. In the long term, state and human security both depend on the promotion of democratic forms of governance, accountable institutions, and the fulfilment of fundamental rights.

Here, security assistance can play a key role by promoting adherence to international legal standards as they relate to surveillance. As more public information has emerged about the technical capabilities used for surveillance, largely instigated by journalists and whistleblowers, or by large-scale examples of abuses of surveillance powers, there have been significant national and international legal challenges against specific practices. This has resulted in an evolving body of jurisprudence on surveillance practices and their lawfulness under international human rights law. Simultaneously, best practices for the governance of surveillance agencies, including their oversight, and the standards for ensuring surveillance is carried out according to principles of necessity and proportionality, as required by international law, have been developed by civil society, academia, and international bodies around the world. State sponsors of surveillance around the world should be prioritising promoting such practices and standards by embedding them into training programmes, conditioning any provision of surveillance on their adherence, and ensuring foreign security authorities are made democratically accountable and operate within the rule of law. Failure to do so, while massively increasing spending on such programmes, will see surveillance being used to not only undermine the rights and physical security of people, but actively undermine democracy, rule of law, and global security.

References

1 “Malaysia 2017 Human Rights Report, Country Reports on Human Rights Practices for 2017” United States Department of State, Bureau of Democracy, Human Rights and Labor. https://www.state.gov/documents/organization/277339.pdf

2 “FBI Shares Tools, Trains Partner Nations to Fight Terrorists Online,” Department of Defense, George C. Marshall European Center for Security Studies, Dec.1, 2017. https://www.defense.gov/News/Article/Article/1385342/fbi-shares-tools-trains-partner-nations-to-fight-terrorists-online/.

3 US Government Accountability Office, ‘Security Assistance: U.S. Government Should Strengthen End-Use Monitoring and Human Rights Vetting for Egypt’ GAO-16-435, April 12, 2016, http://www.gao.gov/products/GAO-16-435 (accessed 09 September 2016)

4 Home Affairs Committee, ‘College of Policing: three years on’, July 2016, para 68 http://www.publications.parliament.uk/pa/cm201617/cmselect/cmhaff/23/2309.htm?utm_source=23&utm_medium=bulletlinks&utm_campaign=modulereports (accessed 09 September 2016)

5 Brown, R & O’Donnell, B, ‘The Un-Freedom Agenda’, Foreign Policy, 2016 <http://foreignpolicy.com/2016/04/20/the-unfreedom-agenda-niger-elections-terrorism (accessed 09 September 2016)

6 Adams, G & Sokolsky, R, ‘Governance and Security Sector Assistance: The Missing Link—Part I’, Lawfare, 2015, <https://www.lawfareblog.com/governance-and-security-sector-assistance-missing-link%E2%80%94part-i (accessed 09 September 2016)

7 Hartung, W, ‘Corruption in Military Aid Undermines Global Security’, LobeLog Foreign Policy, 2016, https://lobelog.com/corruption-in-military-aid-undermines-global-security (accessed 09 September 2016)

8 Watts, S, ‘Identifying and Mitigating Risks in Security Sector Assistance for Africa’s Fragile States’, RAND Corporation, 2015, <http://www.rand.org/pubs/research_reports/RR808.html (accessed 09 September 2016)

9 11’Military and Police Aid by Year’, Security Assistance Monitor, Washington DC, [website] http://securityassistance.org/data/country/military/country/2000/2017/is_all/Global (accessed 08 January 2018)

10 Tarnoff, C & Lawson, M, ‘Foreign Aid: An Introduction to U.S. Programs and Policy’, Congressional Research Service, Washington DC, 2016, p 2

11 Global Trends Forced Displacement in 2016, United Nations High Commissioner for Refugees, 19 June 2017, < http://www.unhcr.org/5943e8a34.pdf>

12 Ibid

13 Malik, N, “Bashir Comes in From the Cold”, Foreign Policy, 31 July 2016, <http://foreignpolicy.com/2016/07/31/europes-new-best-friend-in-africa-is-an-indicted-genocidal-war-criminal/>

14 ‘Commission proposes measures in support of security and development in partner countries’, European Commission, Brussels, 2016, [website] http://europa.eu/rapid/press-release_MEMO-16- 2408_en.htm (accessed 12 September 2016)

15 Northern Atlantic Treaty Organisation, ‘NATO: The First Five Years, 1949-1954’, [website], 2001, http://www.nato.int/archives/1st5years/chapters/3.htm (accessed 09 September 2016)

16 Klare, M & Anderson, A, ‘US and Soviet Military Aid’, in A Scourge of Guns: The Diffusion of Small Arms and Light Weapons in Latin America, Washington, DC, Federation of American Scientists, 1996, pp 27 - 37

17 Klare, M, “The International Repression Trade”, Bulletin of Atomic Scientists, November 1979, p 24

18 Ibid

19 Ibid, p23

20 Ibid, p25

21 Rubenberg, C, ‘Israel and Guatemala: Arms, Advice and Counterinsurgency’, Middle East Report, Washington, DC May-June 1986

22 Federal Bureau of Investigations, ‘Going Dark’, [website] https://www.fbi.gov/services/operational-technology/going-dark (accessed 09 September 2016)

23 Tarnoff, C & Lawson, M, ‘Foreign Aid: An Introduction to U.S. Programs and Policy’, Congressional Research Service, Washington DC, 2016, p 3

24 11’Military and Police Aid by Year’, Security Assistance Monitor, Washington DC, [website] http://securityassistance.org/data/country/military/country/2000/2017/is_all/Global (accessed 08 January 2018)

25 Tarnoff, C & Lawson, M, ‘Foreign Aid: An Introduction to U.S. Programs and Policy’, Congressional Research Service, Washington DC, 2016, p 2

26 ‘Foreign Military Training and DoD Engagement Activities of Interest in Fiscal Years 2016 and 2017: A Report to Congress’, Department of Defense, Department of State, Washington DC, 2015 https://www.state.gov/documents/organization/275295.pdf (accessed 08 January 2018)

27 Bureau of International Narcotics and Law Enforcement Affairs, International Law Enforcement Academies, US Department of State [website] https://www.state.gov/j/inl/focus/combatting/ilea/ (accessed 09 January 2018)

28 from DR Congo, Republic of Congo, Togo, Uganda, Tanzania, Zambia, and Botswana

29 2017 Training Schedule, International Law Enforcement Academy (ILEA) Gaborone, http://www.ileagaborone.com/files/2017_ILEA_Gaborone_Schedule.pdf (accessed 09 January 2018)

30 International Law Enforcement Academy (ILEA) Gaborone Course Catalog, International Law Enforcement Academy (ILEA) Gaborone, http://www.ileagaborone.com/files/ILEA_Course_Catalog-gabs_version.pdf (accessed 09 January 2018)

31 Ibid

32 “Antiterrorism Assistance Program,” Government Accountability Office, October 4, 2017, https://www.gao.gov/products/GAO-17-704.

33 Office of U.S. Foreign Assistance Resources, 2016/Anti-Terrorism Assistance (ATA) Program (Summary), US Department of State, https://www.state.gov/f/evaluations/all/269674.htm (accessed 09 January 2018)

34 Office of U.S. Foreign Assistance Resources, 2013/Morocco/The Anti-Terrorism Assistance Program, US Department of State, https://www.state.gov/f/evaluations/all/232979.htm (accessed 09 January 2018)

35 Office of U.S. Foreign Assistance Resources, 2016/Anti-Terrorism Assistance (ATA) Program (Summary), US Department of State, https://www.state.gov/f/evaluations/all/269674.htm (accessed 09 January 2018)

36 Beckhusen, R, ‘US Looks to Re-Up It’s Mexican Surveillance System’, Wired, 2013

37 ‘INL End Use Monitoring (EUM) Report’, Department of State, Bureau of International Narcotics and Law Enforcement Affairs, Washington DC, 2008, http://www.state.gov/documents/organization/137966.pdf p 36

38 ‘INL End Use Monitoring (EUM) Report’, Department of State, Bureau of International Narcotics and Law Enforcement Affairs, Washington DC, 2008, http://www.state.gov/documents/organization/137966.pdf p 311

39 ‘INL End Use Monitoring (EUM) Report’, Department of State, Bureau of International Narcotics and Law Enforcement Affairs, Washington DC, 2008, http://www.state.gov/documents/organization/137966.pdf p75

40 ‘INL End Use Monitoring (EUM) Report’, Department of State, Bureau of International Narcotics and Law Enforcement Affairs, Washington DC, 2008, http://www.state.gov/documents/organization/137966.pdf p 189

41 Bureau of Counterterrorism and Countering Violent Extremism, Country Reports on Terrorism 2016, US Department of State, Washington DC, https://www.state.gov/j/ct/rls/crt/2016/index.htm

42 Bureau of Counterterrorism and Countering Violent Extremism, Country Reports on Terrorism 2016, US Department of State, Washington DC, https://www.state.gov/j/ct/rls/crt/2016/272234.htm

43 Gillison, D et al, ‘The Network: ‘Leaked Data Reveals How the U.S. Trains Vast Numbers of Foreign Soldiers and Police With Little Oversight’, The Intercept, 2016

44 Ibid

45 “A Global Guide to U.S. Security Aid Programs,” Washington Office on Latin America, April 2017.

46 Ibid.

47 Ibid.

48 2018 Posture Statement to Congress, US Africa Command, 13 March 2018 < http://www.africom.mil/about-the-command/2018-posture-statement-to-congress>

49 “President of Djibouti visits Camp Lemonnier,” AFRICOM press release, November 8, 2017.

50 Office of the Under Secretary of Defense (Comptroller), Counterterrorism Partnership Fund Department of Defense Budget Fiscal Year (FY) 2016, Department of Defense, March 2015, http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2016/FY2016_CTPF_J-Book.pdf (accessed 10 January 2018)

51 ibid

52 US Government Accountability Office, Afghanistan Security: U.S.-Funded Equipment for the Afghan National Defense and Security Forces, https://www.gao.gov/assets/690/686477.pdf (accessed 09 January 2018) p3

53 Ibid p17

54 Report to Congress In Accordance With Section 1225 of the Carl Levin and Howard P. “Buck” McKeon National Defense Authorization Act for Fiscal Year 2015 (P.L. 113-291), as amended, Enhancing Security and Stability in Afghanistan, US Department of Defense, https://www.defense.gov/Portals/1/Documents/pubs/1225-Report-Dec-2017.pdf (accessed 09 January 2018) p88

55 International Criminal Investigative Training Assistance Program, ICITAP Field Offices & Funded Countries, US Department of Justice, https://www.justice.gov/criminal-icitap/file/639486/download (accessed 09 January 2018)

56 International Criminal Investigative Training Assistance Program, About ICITAP, US Department of Justice, https://www.justice.gov/criminal-icitap/file/786726/download (accessed 09 January 2018)

57 Ibid

58 Bureau of Counterterrorism and Countering Violent Extremism, Country Reports on Terrorism 2016, US Department of State, Washington DC, https://www.state.gov/j/ct/rls/crt/2016/272231.htm (accessed 09 January 2018)

59 Foreign Military Training Report, Fiscal Years 2016 and 2017, Joint Report to Congress Volume II, https://www.state.gov/documents/organization/275296.pdf.

60 Abu Ghraib abuses tied to 8 GIs at Huachuca, Tucson Citizen, 31 August 2004, < http://tucsoncitizen.com/morgue2/2004/08/31/137067-abu-ghraib-abuses-tied-to-8-gis-at-huachuca/>

61 “As Army Adds Interrogators, It Outsources Training,” Washington Post, September 23, 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/09/22/AR2006092201486.html.

62 Foreign Military Training Report, Fiscal Years 2016 and 2017, Joint Report to Congress Volume II, https://www.state.gov/documents/organization/275296.pdf.

63 Ibid

64 Ibid

65 “Signal Center of Excellence (SIGCoE) – Fort Gordon,” posted on a website operated by one of the contractors at Fort Gordon, RLM Communications Inc. http://www.rlm-communications.com/contract-vehicles/signal-center-of-excellence-sigcoe/

66 A Joint Audit by the Inspectors General of Department of State and Department of Defense, Afghan National Police Training Program: Lessons learned during the Transition of Contract, DOS Report no. Aud/cG-11-42, 15 August 2011, <https://timemilitary.files.wordpress.com/2011/08/170762.pdf>

67 “AAR wins IDIQ award from US Naval Warfare Command,” AAR press release, February 19, 2018.

68 “Congress worries the contractor flying diplomats around the globe isn’t safe,” The Daily Caller, September 25, 2017, http://dailycaller.com/2017/09/25/congress-worries-the-contractor-flying-diplomats-around-the-globe-isnt-safe/.

69 “PAE awarded State Department Contract for Security and Support Services in Afghanistan,” PAE press release, December 8, 2017, https://www.pae.com/news/press-releases/pae-awarded-state-department-contract-security-and-support-services-afghanistan.

70 “PAE Government Services awarded USD142 million contract to train Afghan forces,” IHS Jane’s Defence Weekly, May 24, 2017, http://www.janes.com/article/70751/pae-government-services-awarded-usd142-million-contract-to-train-afghan-forces.

71 636827 - Fort Huachuca Training And Support Contract (Htasc), LiveCareer, <https://jobs.livecareer.com/l/636827-fort-huachuca-training-and-support-contract-htasc-leidos-38027fc1912902e74163dc0bc7f4a89f>

72 Ibid.

73 Nkala, O, “Tunisia getting $20 million sensor package for border security”, DefenceWeb, 1 March 2018, <http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=50895&catid=74&Itemid=30>

74 Romanian Secret Service Gets €25 Million from EU for Mass Surveillance Project, Liberties, 24 August 2016, < https://www.liberties.eu/en/news/romanian-secret-services-granted-european-fund-for-mass-surveillance/9475>

75 Putting the PNR pieces in place: more EU funding for mass surveillance, Statewatch, 30 March 2016, < http://statewatch.org/news/2016/mar/pnr-interconnection-project.html>

76 European Commission, Instrument contributing to Stability and Peace, [website] https://icspmap.eu (accessed 11 January 2018)

77 European Commission, Deploying expertise to support the Tunisian authorities in the fight against terrorism, [website] https://icspmap.eu (accessed 11 January 2018)

78 Ibid

79 Action Document for 2017-2018 Action Programme of the African Peace Facility, European Commission, http://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-5291-F1-EN-ANNEX-1-PART-1.PDF (accessed 10 January 2018) p6

80 African Union Commission, African Peace and Security Architecture. APSA Roadmap 2016 – 2020, December 2015, http://www.peaceau.org/uploads/2015-en-apsa-roadmap-final.pdf (accessed 10 January 2018)

81 The EU emergency Trust Fund for Africa, European Commission, https://ec.europa.eu/europeaid/regions/africa/eu-emergency-trust-fund-africa_en (accessed 11 January 2018)

82 Baldo, S, Border Control from Hell, Enough, April 2017, https://reliefweb.int/sites/reliefweb.int/files/resources/BorderControl_April2017_Enough_Finals.pdf (accessed 11 January 2018)

83 ibid

84 ‘Third Countries’, Frontex, 2016, [website] http://frontex.europa.eu/partners/third-countries/ (accessed 10 September 2016)

85 Frontex, Frontex cooperation with non-EU countries April 2015-April 2017, https://www.asktheeu.org/en/request/4085/response/13249/attach/3/Frontex%20cooperation%20with%20non%20EU%20countries.pdf (accessed 10 January 2018)

86 European Commission, “A modern budget for a Union that protects, empowers and defends: Questions and Answers”, Press Release, 2 May 2018, < http://europa.eu/rapid/press-release_MEMO-18-3621_en.htm>

87 The European Consensus’, Joint statement by the Council and the representatives of the governments of the Member States meeting within the Council, the European Parliament and the Commission on European Union Development Policy entitled, Official Journal, C 46 of 24.2.2006.

88 ‘Commission proposes measures in support of security and development in partner countries’, European Commission, Brussels, 2016, [website] http://europa.eu/rapid/press-release_MEMO-16-2408_en.htm (accessed 12 September 2016)

89 Chadwick, V, EU to invest in military capacity for development work, Devex, 19 December 2017, https://www.devex.com/news/eu-to-invest-in-military-capacity-for-development-work-91756 (accessed 11 January 2018)

90 Development and humanitarian funding in the post-2020 EU Multiannual Financial Framework, Oxfam, February 2018, < https://d1tn3vj7xz9fdh.cloudfront.net/s3fs-public/file_attachments/oxfam_position_on_the_mff_-_working_doc.pdf>

91 Tobias Ellwood MP, Reponse to written question 64841, House of Commons Hansard, 01 March 2017, http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2017-02-21/64841/ (accessed 10 October 2017)

92 British Embassy Kyiv, UK programme assistance to Ukraine 2016-2017, 26 January 2017, https://www.gov.uk/government/news/uk-programme-assistance-to-ukraine-2016-2017 (accessed 11 January 2018)

93 Ibid

94 Miller, P, “Exclusive: Secret Documents Reveal How Britain Funded Possible War Crimes in Sri Lanka”, 31 March 2016, Vice, < https://www.vice.com/en_uk/article/dp5beq/sri-lanka-british-police-training-phil-miller>

95 Vallance, C, ‘Torture fears as British police train Saudis’, BBC, 2016 http://www.bbc.co.uk/news/uk-36468268 (accessed 09 September 2016)

96 Home Affairs Committee, ‘College of Policing: three years on’, July 2016, para 77 http://www.publications.parliament.uk/pa/cm201617/cmselect/cmhaff/23/2309.htm? utm_source=23&utm_medium=bulletlinks&utm_campaign=modulereports (accessed 09 September 2016)

97 23Ibid, para 69

98 Monroy, M & Mortada, L, German police cooperation with Egypt: New security agreement takes effect, November 2017, https://digit.site36.net/2017/11/14/police-cooperation-with-egypt-new-security-agreement-takes-effect/ (accessed 10 January 2018)

99 Naceur, S, ‘Is Germany an Accessory to Repression?’, Qantara, 2016, https://en.qantara.de/content/police-co-operation-with-egypt-is-germany-an-accessory-to-repression

100 Monroy, M & Mortada, L, German police cooperation with Egypt: New security agreement takes effect, November 2017, https://digit.site36.net/2017/11/14/police-cooperation-with-egypt-new-security-agreement-takes-effect/ (accessed 10 January 2018)

101 ‘La formation en sécurité intérieure’, French Ministry of Foreign Affairs and International Development, 2013, [website] http://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/defense-et-securite/cooperation-de-securite-et-de-defense/les-ecoles-nationales-a-vocation- regionale/article/la-formation-en-securite (accessed 09 September 2016)

102 Bagnoli, L, Civipol, la multinazionale francese che vende sicurezza in Africa, La Stampa, May 2017, http://www.lastampa.it/2017/05/24/esteri/speciali/divertedaid/civipol-la-multinazionale-francese-che-vende-sicurezza-in-africa-xwOPuGCSbcpSzBTNs17diM/pagina.html (accessed 10 January 2018)

103 Coca, N, “China’s Xinjiang Surveillance is the Dystopian Future Nobody Wants”, Engadget, 22 February 2018.

104 “China’s Xi pledges security equipment, training for Afghanistan”, Reuters, 10 July 2015

105 Sacks, S, “Beijing Wants to Rewrite the Rules of the Internet”, The Atlantic, 18 June 2018, <https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/>

106 Wade, S, “Chinese Surveillance Tech, from Xinjiang to S. America”, 23 January 2018, China Digital Times, <https://chinadigitaltimes.net/2018/01/chinese-surveillance-tech-xinjiang-south-america/>

107 Joplin, T, “China’s Newest Global Export? Policing Dissidents”, Al Bawaba, 31 May 2018, <https://www.albawaba.com/news/china’s-newest-global-export-policing-dissidents-1139230>

108 Khan, I, “Chinese Firm to Provide Equipment for Safe City Project”, Dawn, 22 March 2014

109 ‘The Five Eyes’, Privacy International, London, 2015, [website] https://www.privacyinternational.org/node/51 (accessed 14 September 2016)

110 Gallagher, R, ‘Inside Menwith Hill’, The Intercept, 2016 https://theintercept.com/2016/09/06/nsa- menwith-hill-targeted-killing-surveillance/ (accessed 16 September 2016)

111 Campbell, D, ‘NSA: Inside the FIVE-EYED VAMPIRE SQUID of the INTERNET’, The Register, 2014, http://www.theregister.co.uk/2014/06/05/how_the_interenet_was_broken/ (accessed 15 September 2016)

112 Gallagher, R, ‘How Secret Partners Expand the NSA’s Surveillance Dragnet’, 2014, The Intercept, https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/ (accessed 15 September 2016)

113 Campbell, D, ‘NSA: Inside the FIVE-EYED VAMPIRE SQUID of the INTERNET’, The Register, 2014, http://www.theregister.co.uk/2014/06/05/how_the_interenet_was_broken/ (accessed 15 September 2016)

114 Campbell, D, ‘REVEALED: GCHQ’s BEYOND TOP SECRET Middle Eastern INTERNET SPY BASE’, The Register, 2014, http://www.theregister.co.uk/2014/06/03/revealed_beyond_top_secret_british_intelligence_middlee ast_internet_spy_base/ (accessed 15 September 2016)

115 Turse, N, ‘How the NSA Built a Secret Surveillance Network for Ethiopia’, The Intercept https://theintercept.com/2017/09/13/nsa-ethiopia-surveillance-human-rights/ (Accessed 08 January 2018)

116 Gallagher, R, Japan Made Secret Deals With the NSA That Expanded Global Surveillance, The Intercept, 24 April 2017, https://theintercept.com/2017/04/24/japans-secret-deals-with-the-nsa-that-expand-global-surveillance/ (accessed 12 January 2018)

117 See, for example, Fioretti, J, EU Court Says Mass Data Retention Illegal, Reuters, December 2016, Savage, C, & Weisman, J, N.S.A. Collection of Bulk Call Data Is Ruled Illegal, New York Times, 7 May 2015, Gallagher, R, In Historic Ruling, UK Surveillance Secrecy is Ruled Illegal, The Intercept, 6 February 2015

118 See, for example, Miller, N, ‘The Leahy Law: Congressional Failure, Executive Overreach, and the Consequences’, Cornell International Law Journal 667, 2012

PRIVACY INTERNATIONAL

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471