Defining Remote Warfare: Intelligence Sharing after 9/11

Briefing Number 5

Prof. Julian Richards

Oxford Research Group
Remote Warfare Programme

This report has been commissioned by the **Oxford Research Group's Remote Warfare Programme,** formerly known as the Remote Control Project. We were set up in 2014 to examine changes in military engagement, with a focus on remote warfare. This is the trend in which countries like the United Kingdom choose to support local and regional forces on the frontlines rather than deploying large numbers of their own troops.

Published by Remote Warfare Programme, October 2018.

Cover image: City Lights 2012 (NASA image acquired April 18 - October 23, 2012).

Remote Warfare Programme
Oxford Research Group
Development House
56-64 Leonard Street
London EC2A 4LT
United Kingdom
+44 (0)207 549 0298

org@oxfordresearchgroup.org.uk

http://oxfordresearchgroup.org.uk

About the Series

The *Remote Warfare Programme* is a research and policy unit analysing the rise of remote warfare: the recent shift away from "boots on the ground" deployments towards light-footprint military interventions abroad.

Among other factors, austerity, budget cuts, war-weariness, and high political risk aversion in the wake of Iraq and Afghanistan have all played their part in making large-scale UK military deployments less palatable to the UK Parliament and public.[1]

Alongside this, trends in military engagement such as the increasing use of drones and an increased focus on counterterrorism and building local capacity – evident in, for example, the addition of defence engagement as a core task of the Ministry of Defence – have allowed the UK to play a role in countering threats posed by groups like Islamic State, Boko Haram, al-Qaida and al-Shabaab without deploying large numbers of its own troops.

The emergence of approaches that seek to counter threats at a distance, without the deployment of large military forces, is an umbrella definition of remote warfare. With local troops engaged in the bulk of the frontline fighting, the UK's role has, by and large, been a supporting one, providing training and equipment and, where necessary, providing air and intelligence support, and the assistance of UK Special Forces to bolster local troops.

The focus of the *Remote Warfare Programme*'s work has been on a strategic level, asking what the implications of these changes in military engagement are for the transparency, accountability and effectiveness of UK military engagement abroad.[2]

However, to ask these strategic questions, we have often had to put to one side the fact that remote warfare is not an uncontested term, and our broad definitions and analysis often hinge on an assumption that "you know it when you see it". Moreover, while we have been focusing on the use of remote warfare on today's battlefield, we are also aware that future changes in technology, especially the rising importance of cyber, will have an impact on how we should understand remote warfare.

This series brings together experts to discuss important aspects of remote warfare to provide some conceptual clarity. It looks at current practice, including reports on security cooperation, intelligence sharing, private security companies and drones, as well as looking to the future of warfare: addressing how offensive cyber operations could change the landscape of military engagement.

Over the course of the past year, we have been releasing bi-monthly briefings on these subjects by experts in their field, with the eventual aim of exploring common themes, risks and opportunities presented by the evolving use of remote warfare.

About this briefing

Remote warfare is underpinned by a complex web of intelligence sharing between partners. In a world characterised by complex transnational threats, the logic of such sharing is difficult to dispute. At the same time, considerable risks are present in ensuring that human rights abuses and compromises to the right to privacy are not realised by multilateral intelligence sharing. This paper considers the state of play of intelligence sharing in contemporary remote warfare, and the degree to which the benefits of sharing are balanced by the mitigation of risk.

Author bio

Professor Julian Richards spent nearly twenty years working for the British government in intelligence and security policy, before co-founding the Centre for Security and Intelligence Studies (BUCSIS) at the University of Buckingham. His research interests include intelligence machinery and governance; and counter-terrorism policy in a range of regional and global contexts.

Contents

Abbreviations

BND	Bundesnachrichtendienst (Federal Intelligence Service), Germany
CG	Consolidated Guidance
CIDT	Cruel, Inhuman and Degrading Treatment
EITs	Enhanced Interrogation Technique
FCO	Foreign and Commonwealth Office
GCHQ	Government Communications Headquarters
GWOT	Global War on Terror
HRW	Human Rights Watch
IPA	Investigatory Powers Act
IPCO	Investigatory Powers Commissioner's Office
IPT	Intelligence Powers Tribunal
ISA	Intelligence Services Act
ISC	Intelligence and Security Committee
ISI	Inter-Services Intelligence Directorate
MI5	Security Service
MI6	Secret Intelligence Service
MOU	Memorandum of Understanding
NATO	North Atlantic Treaty Organisation
NDS	National Directorate of Security
NGO	Non-Governmental Organisation
NSA	National Security Agency
Sigint	Signals intelligence
SSA	Security Service Act
UNSC	United Nations Security Council

Introduction

In the post-9/11 period, the logic of remote warfare for Western powers has been greatly enhanced by the challenging and transnational nature of terrorist and criminal movements, and by a growing Western fatigue with fatalities amongst its own troops. Increasing budgetary pressures on military expenditure and the drive to "achieve more with less" are also undoubtedly increasing the lure of remote warfare. But these developments have also come with a cost in terms of pitfalls in ethics and legality.

Intelligence sharing can greatly enhance operations in this new landscape, both by achieving intelligence and security objectives through the receipt of information from partners; and by underpinning the capacity of those partners by investing in their intelligence gathering capabilities. The basic logic of intelligence sharing is difficult to dispute. Indeed, in response to the threat posed by violent extremists returning from conflicts such as those in Iraq and Syria (the "foreign fighters" problem), the UN Security Council (UNSC) recently passed Resolution 2396, reminding Member States of their collective obligations to confront the threat of terrorism. The resolution mandated that:

> *Member States to improve timely information sharing, through appropriate channels and arrangements, and consistent with international and domestic law, on foreign terrorist fighters, especially among law enforcement, intelligence, counterterrorism, and special services agencies, to aid in determining the risk foreign terrorist fighters pose, and preventing them from planning, directing, conducting, or recruiting for or inspiring others to commit terrorist attacks*.[3]

Thus, for a state such as Britain in the contemporary age, working more intensively with intelligence partners makes sense. But the key questions are whether doing so can be properly monitored and regulated, such that serious human rights abuses are not committed by local partners. This may be a question in any relationships with partners, but experience has shown it can also be a problem in the relationship with the largest and most important intelligence partner, the US.

This paper examines the way in which intelligence sharing has the potential to exacerbate the risks inherent in remote warfare. The first risk is that, if done badly, sharing of intelligence can sometimes look like "outsourcing" of legally and ethically dubious activities to those states who do not share the same standards of human rights and democratic accountability in their pursuit of national security. The more partners the UK deals with and the worse their respective histories of human rights compliance, the greater the challenges faced in convincing others that security is being delivered in a democratic, accountable and ethical way.

…in the contemporary age, working more intensively with intelligence partners makes sense. But the key questions are whether doing so can be properly monitored and regulated

The second risk is that shared human intelligence or communications data will be used to conduct unlawful, unethical or disproportionate targeting operations in various parts of the globe. The risk is that shared intelligence will trigger abuses of human rights in ways that cannot be properly monitored. Connected to this risk is that of the "bulk" sharing of intercepted material, as Edward Snowden revealed was happening between the US and multiple allies, including the UK. In this realm, one of the pitfalls is that highly complex and integrated signals intelligence (Sigint)

systems sharing ever more industrial-scale amounts of data, could allow for national laws on privacy and surveillance to be circumvented by covertly utilising material intercepted by partners. In this sense, the human right in sharp focus here is that of the right to privacy.

Added to these problems is the fact that oversight of intelligence has been difficult. Intelligence sharing relationships are often among the most sensitive aspects of any intelligence agency's activities. For this reason, they are usually shrouded in secrecy, not only from the public but occasionally from the relevant agency's own oversight bodies.

This analysis begins by considering the risks associated with a broad set of intelligence sharing partnerships in the contemporary remote warfare environment. In particular, it will consider how differing conceptions of national security, and perceptions around how to achieve it across the globe, can lead to problems in intelligence relationships. The question of industrial-scale communications data-sharing with partners is also considered, in terms of the difficulties in ensuring compliance with human rights obligations in such an automated environment.

The discussion then moves on to the particular context of the early years of the so-called Global War on Terror (GWOT), in which standing shoulder-to-shoulder with the US posed an especially challenging set of questions for Britain and its national security posture.

Many of the problems in these years have only come to light recently with the publication of the Intelligence and Security Committee's (ISC) Inquiry report on Detainee Mistreatment and Rendition. The findings of this report are scrutinised in detail in the third and final section. The conclusions will offer an overall assessment of how far intelligence sharing has led to abuses in the past, and whether it is likely to do so in the future.

Key terms: Intelligence sharing partnerships and agreements

- **The "Five Eyes" relationship** (encompassing intelligence sharing between the US, UK, Canada, Australia and New Zealand), struck at the end of the Second World War and still going very strong, is probably the deepest and most formalised multi-partner intelligence relationship in global history.
- **The Club of Bern** constitutes a less formal relationship between Western security agencies, its membership closely mirroring that of NATO.
- Beyond these two, most other intelligence sharing relationships are bilateral, focused on particular "compartmented" activities, and are less openly documented.
- **Memoranda of Understanding (MOUs)** sometimes apply to intelligence relationships and intelligence agreements between two partners, they are specified but are often consciously avoided when attempting to establish trust with partners.
- The **"third party" rule** is a universally-accepted protocol that shared intelligence will not be used or disseminated further without the originator's agreement. But onward sharing is not always visible, and the agreement is essentially based on trust.
- Occasionally, covert infiltration of an intelligence partner by a hostile agency can cause shared intelligence to be leaked.
- With partners for whom historic human rights abuses of detainees can be an issue, **"diplomatic assurances"** are sometimes received through the consular office. However, human rights NGOs such as Human Right Watch (HRW) have often dismissed such assurances as worthless.

Supping with a long spoon: risks in intelligence collaboration

Different conceptions of national security

Most non-Western states do not have clearly delineated and articulated expressions of their national security objectives, such as those seen in the UK's National Security Strategy.[4] This is because national security is a very simple and straightforward affair in these states and revolves around two core objectives: ensuring the territorial integrity of the state; and guaranteeing the continued survival of the regime. Most do not have any legislation governing the scope or modus operandi of their intelligence and security agencies, and many have severely lacking or compromised mechanisms for parliamentary scrutiny of their activities. There is a direct link here with democracy, whether it is lacking or dysfunctional in the state in question.

As the former Director-General of both the Inter-services Intelligence (ISI) and Military Intelligence in Pakistan, Lt. General Asad Durrani described "[Intelligence agencies] have to use unconventional means. And, to neutralize similar methods by the other side, they will be seriously handicapped if they were to strictly operate under the law".[5] Pakistan, it should be noted, has been under military rule for approximately half its existence, and the military and ISI intelligence agency remain the most important wielders of power even in times of civilian government. This can lead to a particularly repressive and non-democratic national security culture, which is replicated in many other states, particularly those with similar histories of military rule.

Related to this is the perception of Islamist movements in the Middle East. Hassan al-Banna, the founder of the Muslim Brotherhood in Egypt, recognised right from the start that a grass-roots popular Islamist movement would be seen as a threat to power by the military establishment and would accordingly be repressed at every turn.[6] While he saw this as a cause for militant resistance, his prediction was correct not only in Egypt but also across the Middle East, where military regimes and unelected monarchies alike have been happy to repress Islamist movements that are seen as a fundamental threat to the regime's survival.

The problem for Western countries in establishing intelligence relationships more widely is that, while both sides might share basic counter-terrorist operational objectives, the underlying conception of national security may be different, and sometimes dangerously so. This problem can often manifest itself in the partner country wishing to obtain intelligence on expatriate dissident movements rather than on "terrorists" per se. For the UK, where London has been lambasted in the past as a "Londonistan" for harbouring the world's most dangerous radicals and dissidents,[7] this can be an attractive element for countries that wish to obtain intelligence on London-based political oppositionists. Martin Rudner of Carleton University describes how the Egyptian and Jordanian governments have both complained to the UK about its failure to supply them with intelligence on dissidents residing in London,[8] while Elizabeth Sepper of the Columbia Law School describes the case of the Libyan authorities being able to interrogate detainees at Guantanamo Bay about Libyan dissidents in the UK.[9]

Conversely, intelligence provided to such countries on purported terrorist targets can lead to violent actions being taken on the ground, violating human rights and neutralising potential further sources of intelligence.

Partners such as Israel can pose a particular set of difficult questions for Western intelligence agencies. Israel's undoubtedly

highly advanced technical and military capability and their pro-Western stance within an otherwise hostile region, must be carefully balanced against an avowedly robust and uncompromising approach to national security. Israeli national security policy involves the deployment of covert intelligence and military action where it feels it is threatened. After 1981, the US slowed the flow of intelligence to Mossad after the Israelis had purportedly used their information to destroy Iraq's nascent nuclear reactor in a pre-emptive military strike.[10] More recently, heavy military actions against Hamas and Hezbollah within the Occupied Territories continue to place Israel's Western military and intelligence partners in uncomfortable positions concerning complicity with disproportionate military action in civilian areas.[11]

In many situations, war and violent counter-insurgency operations may cause especially difficult questions to be asked not just in terms of the use of military equipment being supplied to repressive regimes but also to the tactical use of intelligence. In the ongoing civil war in Yemen, for example, the US has come under increasing pressure to curb military and intelligence support to Saudi Arabia following destructive bombing that has caused considerable civilian casualties,[12] not to mention a looming humanitarian catastrophe affecting much of the population. The UK's own assistance beyond arms sales is unclear. It has long been claimed that intelligence provided by the Kingdom has foiled terrorist attacks against British civilians and there have been some indications that intelligence is provided the other way.[13] Similarly, Britain's MI6 and Special Forces have also been implicated in supplying geolocational intelligence to the Americans to facilitate drone strikes by forces in the region.[14] While Yemen has been a key source of intelligence on al-Qaida in the Arabian Peninsula in the past, the reciprocal cost for civilians in the region can turn out to be high.

A meeting at the UN Security Council (image credit: US Department of State/ Flickr, 2014).

More widely, Western states such as the UK, the Netherlands, Germany and Italy have been closely involved with the US' global system of drone strikes against terrorist high-value targets. Such assistance has included not only geolocational data on targets of interest, but also electronic infrastructure support and the use of air-bases in their territories from which to launch the strikes.[15]

Human Rights

The most important questions to arise from the immediate post-9/11 years were whether and, if so, how Western intelligence partners had either been complicit in the use of intelligence derived from cruel, inhuman or degrading treatment (CIDT), or had indeed committed abuses themselves in the case of the US' use of "enhanced interrogation techniques" (EITs) in Guantanamo Bay and elsewhere. From the UK's perspective, this issue received extensive treatment in the ISC's inquiry into Detainee Mistreatment and Rendition, considered at length below, although a number of other cases have also come to light.

Officially, the UK makes a great deal of its mission to uphold values in its foreign policy.

The latest UK National Security and Capability Review states that:

> *The rules-based system we helped to develop has enabled global cooperation to protect shared fundamental values of respect for human dignity, human rights, freedom, democracy and equality. As a permanent member of the United Nations Security Council, a leading contributor to [North Atlantic Treaty Organisation (NATO)], a European country sharing fundamental values with our partners and a champion of the Commonwealth, we are committed to upholding and renewing the rules-based international system.* [16]

On the occasion of the 2017 International Day in Support of Victims of Torture, the Foreign and Commonwealth Office (FCO) Minister for Human Rights, Lord Ahmad, noted that:

> *The UK government condemns torture in all circumstances, and I call on governments around the world to eradicate this abhorrent practice.*
>
> *We are continuing to work hard to combat torture, including supporting [Non-Governmental Organisation (NGOs)] to undertake independent monitoring and inspection of places of detention.*
>
> *I urge states that have not yet done so to sign, ratify and implement the UN Convention Against Torture and its Optional Protocol. By taking this step, countries will be making a clear statement about their commitment to end torture and to deliver justice to victims of torture and their families.* [17]

The 1984 Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment expressly outlines an extra-territorial statement of inadmissibility of evidence in court where that evidence has been obtained through the use of CIDT[18]. While the UK may well respect this with its own actions, it cannot be so certain that its partners will do the same, especially when current struggles with violent terrorist networks or wider counter insurgencies may impact what partners consider necessary and appropriate to protect their national security.

From an intelligence perspective, the dilemma is the much-discussed paradox of "dirty hands".[19] As Derek Reveron of the US Naval War College noted, the challenge for Western states is to gain as much tactical intelligence as they can from partner states without becoming "tainted by their tactics".[20]

For Western states dealing with intelligence partners who have a poor record in this area, this poses extremely difficult questions. In post-9/11 Afghanistan, one of the key pillars of security sector reform was the re-establishment of the main intelligence agency, renamed the National Directorate of Security (NDS). It soon became apparent, however, that the ghost of Afghanistan's dark history of oppression, typified by the brutal practices of the communist-era Khadamat-e Aetla'at-e Dawlati state intelligence agency, was rearing its head. In 2007, Amnesty International issued a damning report cataloguing human rights abuses in Afghanistan and highlighting International Security Assistance Force (ISAF)'s alleged complicity in the abuse. Much of it centred around the NDS' notorious "Department 17" facility in Kabul, which received and processed detainees handed over by ISAF for interrogation.[21] In 2012, the peace activist Maya Evans was successful in a judicial review that placed a temporary moratorium on detainee handovers.[22]

Aside from problems in Afghanistan, the UK has experienced a number of controversial cases involving intelligence partners in the post-9/11 period. One of the more significant was the case of Binyam Mohamed, an Ethiopian national who had

formerly been a resident in the UK. In April 2002, Mohamed alleges that he was arrested in Pakistan on terrorist charges and was subsequently mistreated over a period of three months.[23] He claims that a British official who interviewed him over this period told him he was going to be tortured. In July 2002, he was allegedly subjected to an extraordinary rendition to Morocco, where he claims he suffered abuse while facing questions based on information from the British government. He was then moved to Guantanamo Bay, where he was subjected to further episodes of mistreatment.[24] In 2010, the government announced that it had settled out of court with Mohamed and fifteen other former Guantanamo detainees, twelve of whom had launched legal action against the heads of MI5 and MI6. The sum of the settlement was not disclosed but the then-Justice Secretary, Ken Clarke, said at the time of the announcement that the action was necessary to avoid a legal case that could have cost up to £50 million.[25] Thus, it could be said that considerable reputational and material cost for the British government resulted from the case.

At around the same time that Mohamed was being moved from Morocco to Guantanamo Bay, a Libyan dissident opposed to the country's leader, Colonel Muamar Gadhafi, by the name of Abdel Hakim Belhaj, was abducted by the Central Intelligence Agency (CIA) in Thailand and turned over to the Libyan authorities, along with his pregnant wife. It is alleged that the CIA obtained the intelligence on Belhaj's whereabouts from British intelligence, who were working with the Gadhafi government at the time as part of the general GWOT coalition against Islamist extremists.[26]

The subsequent brutal torture of Belhaj by the Libyans, some of it conducted within earshot of his wife, was revealed following the collapse of the Gadhafi government in 2011 and a campaign by HRW on behalf of Belhaj's family. A claim against the British government for £1 in compensation and a full apology was eventually settled on 10 May 2018, when the Attorney General read a statement addressed to Belhaj on behalf of the Prime Minister, saying:

> *On behalf of her majesty's government, I apologise unreservedly… what happened to you is deeply troubling. It is clear that you were subjected to appalling treatment and that you suffered greatly … We should have understood much sooner the unacceptable practices of some of our international partners. And we sincerely regret our failures. We shared information about you… we should have done more to reduce the risk that you would be mistreated. We accept this was a failing on our part. Later, during your detention in Libya, we sought information about and from you. We wrongly missed opportunities to alleviate your plight: this should not have happened.* [27]

In Binyam Mohamed's case, the problems were both with the key intelligence relationship with the Pakistanis, and with the relationship with the US, under whose urging Mohamed was rendered to a third country with a highly dubious record on human rights,[28] eventually ending up in the US' own facility at Guantanamo Bay. As with Mohamed, Belhaj's case also involved the intelligence relationship with the US, who shared the UK's desire to gather intelligence on potential al-Qaida networks. In both cases, the defining features were a willingness to work with unsatisfactory regimes to achieve the results; and a British complicity with clear evidence of mistreatment of detainees through a desire not to disrupt the key intelligence relationship with the US.

A few years later, the UK faced another difficult case of a slightly different hue, when two men were convicted of the brutal murder of an off-duty British soldier, Lee Rigby. It subsequently emerged during an investigation into the case by the ISC that, prior to the attack, one of the perpetrators,

Michael Adebolajo, had submitted a report during a port-stop interview on return to the UK from Kenya that he had suffered serious abuse at the hands of the Kenyan police. At the interview in November 2010, Adebolajo alleged that he had been beaten, and threatened with electrocution and rape on more than one occasion during detention in Kenya.[29]

Leaving aside Adebolajo's subsequent conviction for murder, the allegations highlighted some difficult questions for the British intelligence machinery on whether and how such allegations involving a partner country are investigated, and whether the UK is effectively complicit in mistreatment if one of its intelligence partners commits the wrongdoing. The case also uncovered the fact that MI6 generally accept assurances they are given by intelligence partners that basic compliance with human rights will be observed.

The second concern in the Adebolajo case was that MI6 claimed it was not their responsibility to investigate if allegations of mistreatment in-country arose following receipt of diplomatic assurances. Instead, they claimed, such allegations should be the responsibility of the consular office.[30] This highlights two issues. Firstly, MI6's record-keeping on allegations of mistreatment by intelligence partners was found to be less-than-ideal: there were at least 13 allegations concerning the Kenyan partners similar to those raised by Adebolajo, about which the ISC could only be given patchy and incomplete records.[31] The assumption is that such allegations would be investigated by the consular office, if at all. Secondly, MI6 officers revealed that it is the assumption that terrorist detainees will routinely make allegations of mistreatment on arrest, since this is part of the training they receive from their jihadist sponsors.[32] While there is probably more than a kernel of truth in this, it does lead to a situation of potential jeopardy in which *any* allegations of mistreatment can be instantly dismissed.

The third major area of risk highlighted by the Adebolajo case was the question of which intelligence has been potentially derived from torture when there are multiple agencies working together, and where intelligence is pooled in such a way that the provenance of individual pieces of information may be difficult to ascertain. In the Kenyan case, MI6 work with a multi-agency body of security agencies in-country working on counter-terrorism, including, police, state intelligence and military, and the possibility that some of the intelligence being pooled may have been derived from mistreatment of detainees is more difficult to establish than if the relationship was with one specific agency. This is a significant ongoing area of risk highlighted by the chair of the ISC,[33] and discussed more widely below in the context of the Detainee Mistreatment and Rendition inquiry.

"Big Data"

The principle of national security in those states observing the European Convention of Human Rights (ECHR), enshrined in the UK within the 1999 Human Rights Act, is that states can take extraordinary measures to derogate from some aspects of human rights where there are specified and compelling national security reasons to do so. This includes the right to privacy, allowing for surveillance in specific circumstances, but only in accordance with national laws on the warranting of such a derogation, and in a

GCHQ Building (image credit: Defence Images/ Flickr, 2008).

way that strictly applies the principles of "necessity and proportionality".

The advent of "Big Data" (which means both a massively increased amount of available data on citizens' activities but also increasingly sophisticated technology for databasing, mining and extracting value from such data) has delivered a complex set of opportunities and risks for the major intelligence services. Concerning partnerships, improving technology has increasingly allowed for industrial-scale pooling and cross-referring of major data collections spanning global communications, by linking-together the Sigint systems of partners.

Edward Snowden's revelations in 2013 revealed the depth and complexity of such arrangements, and particularly those between the pre-eminent Sigint agency in the world, the National Security Agency (NSA), and its closest intelligence partners. One of the NSA systems revealed by Snowden was RAMPART-A, which appears to be an international network of interception capabilities against trunk fibre-optic cables carrying the bulk of the global communications network.[34] Leaked to the Danish newspaper, *Dagbladet Information*, the details revealed a data-sharing infrastructure between the NSA and a number of "third-party" intelligence services, namely those in countries outside of the traditional Five-Eyes Sigint agreement. Indeed, the article revealed 33 such third-party Sigint relationships.[35]

Again, there is not necessarily any problem with such an arrangement if it is used to deliver beneficial and ethical national security outcomes. But, as the civil rights NGO, Privacy International noted, there are three potential problems with current arrangements: maintaining the basic human right to privacy; the risk of data being used to commit abuses; and the question of how to make it adequately accountable.[36]

The right to privacy

First is the question of the basic human right to privacy, which, under international human rights law, is extra-territorial. With such industrial-scale interception and databasing of private communications; and their automated sharing between a range of partner states, it is difficult to see how necessity and proportionality can always be knowingly applied to the exploitation of any one individual's communications amongst the morass of data.

There is also a related question that, legally, states participating in such schemes will tend to include in their surveillance legislation and procedures some privacy protections for their own nationals, and for particularly sensitive interest-groups in society such as lawyers, doctors and journalists. But whether and how these are applied to foreign nationals is usually not clear. Indeed, Germany is one of the few countries that has taken steps to address this particular issue. Snowden's revelations led to an ad hoc cross-parliamentary inquiry, called the "NSA Inquiry" (*Untersuchungsausschuss*, NSA) launched in March 2014. This inquiry uncovered concerns and weaknesses in the authorisation process for Sigint collection by the *Bundesnachrichtendienst* (BND), particularly about bulk data collection against foreign nationals, including close EU partners. The outcome was a set of legislative changes governing the activities of the BND, which were completed by 2016.

The problem with a lack of clarity in this area, is not only that the right to privacy of foreign nationals may not be clearly respected by such large-scale data networks, but also that there is a risk that one of the partners in the arrangement could attempt to circumvent their own national restrictions on interception by freely accessing data collected by a partner country, to whom the same laws would not apply. The UK is one of the few countries where a legal challenge to this effect has been undertaken, in the shape of a case brought to the Investigatory

Powers Tribunal (IPT) by Privacy International against Government Communications Headquarters (GCHQ) in 2013, following Snowden's revelation about UK access to an NSA system called PRISM.[37] The results of this case were mixed. The ISC undertook a detailed investigation of GCHQ but found no evidence that they had been circumventing UK law protecting the privacy of UK nationals by accessing NSA's system.[38] At the same time, GCHQ was censured for not having any available guidelines on the operation of its access to PRISM, which technically made such activities unlawful until the time of the IPT's case and GCHQ's formal response in 2014.[39]

Meanwhile, the UK's general law governing interception and surveillance has also been the subject of a court case initiated by coalition of politicians across the major political parties, and a range of civil rights NGOs. The case was initially brought against the human rights protections offered by the 2014 Data Retention and Investigatory Powers Act (DRIPA), and subsequently applied through appeal to the following Investigatory Powers Act (IPA) of 2016. In a landmark case, the European Court of Human Rights (ECHR) has eventually upheld on appeal the original decision of the UK High Court, that the IPA essentially violates privacy rights by their being "insufficient oversight" of the targeting and collection process.[40] The ruling represents an as-yet unresolved conundrum for the Home Office (although it is interesting that the ECHR also ruled that there were no particular concerns to answer about the sharing of surveillance data with foreign governments).

Risk of abuses

The second concern with bulk data-sharing is similar to that concerning arrangements with joint intelligence centres, namely that there is a heightened risk of data being used to commit abuses by a participating country in ways that cannot be easily traced back to any specific piece of information. When data is pooled in huge databases, it is not always easy or possible to conduct an audit trail between an original piece of data and a security outcome.

Amnesty International has outlined a set of concerns about intelligence sharing arrangements between a set of European countries and the CIA in the facilitation of lethal drone strikes.[41] In 2011, a parliamentary inquiry was launched in Germany into the circumstances that had led to the killing of a German citizen in Pakistan by a drone-launched missile, and the potential complicity of the German intelligence services in such strikes. Media reports subsequently identified the degree to which the German military and the national intelligence service, the BND, regularly supply bulk data on communications events to their ISAF partners in Afghanistan and elsewhere in facilitating lethal drone strikes.[42] Given the number of non-combatant collateral casualties in such strikes, there is an ongoing debate as to whether such activities are legal under international law.

In the Netherlands, meanwhile, Snowden's revelations caused a controversy over the interaction between the Dutch anti-piracy operations off the coast of Somalia and the US' intelligence operations against the terrorist group, al-Shabaab. Reports suggest that the Dutch had supplied 1.8 million metadata records of telephone communications to the US from its own interception facilities.[43] The revelation of the scale and complexity of the exchange has triggered a comprehensive inquiry by the parliamentary oversight body, the Review Committee on the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten*, CTIVD). Indeed, legal challenges concerning intelligence assistance to the US in facilitating lethal drone strikes have been launched in several of the US's European intelligence partner countries.[44]

MQ-9 Reaper (image credit: US Air Force, 2015).

Adequately accountable

The final concern in this area is the question of how accountability can be adequately delivered when intelligence services are sharing such volumes of data so routinely. For example, if it transpires that some of that data has been used to affect a repressive or illegal outcome, such as a drone strike killing a number of non-combatants, who should be held accountable and how? It may not be good enough to rely on generalised assurances that all parties will act appropriately: a problem very similar to that of information sharing in the human intelligence sphere with joint counter-terrorism units. It may be the case that, as the volume and rapidity of bulk automated data-sharing systems inexorably increase, such problems will become ever harder to resolve.

As noted above, Germany is possibly the only country where intelligence sharing relationships are explicitly mentioned in law, following the passing of a new act in 2016.[45] Yet even here, it does not seem to offer much clarity on how the BND or its oversight bodies will be able to adequately identify where intelligence sharing arrangements have led to potential legal issues such as abuses of human rights. In the view of one commentator, the recent legislative changes in this area in Germany did "not fix the country's woefully inadequate judicial oversight system",[46] and have even managed to introduce new confusions and gaps in the oversight machinery, leaving parliamentary oversight of intelligence somewhat "fragmented".

Oversight, the ISC, and the Detainee Mistreatment and Rendition Inquiry

The Intelligence and Security Committee (ISC)

Intelligence sharing with partners is just one part of the overall machinery of a state's intelligence function. One of the key questions for democratic states is whether and how the intelligence function can be overseen by parliament and by civil society and can be held accountable for mistakes and abuses.

In the post-Cold War era, most advanced states have instituted laws and oversight mechanisms to greatly increase public scrutiny of their intelligence services, following the long years of espionage and secrecy that characterised the Cold War. It is also arguably the case that civil society has become stronger and more robust in its challenges to the state and its covert activities. In countries such as the UK, for example, it is now commonplace for the heads of the intelligence services to give statements to the press, when their very identity would have been hidden before, and for detailed investigations to be held into intelligence operations and intelligence failures.

The Security Services Act of 1989, and the Intelligence Services Act (ISA) of 1994, both placed the UK's main intelligence services on the statute books at previously unprecedented levels of detail in terms of their remit and function. The 1994 ISA also created the parliamentary Intelligence and Security Committee (ISC), and the complaints tribunal, the Intelligence Powers

Tribunal (IPT). In addition to parliamentary oversight, various commissioners oversee the day-to-day activities of the intelligence services, combined into one Intelligence Powers Commissioner's Office (IPCO) with the passing of the Investigatory Powers Act (IPA) in 2016.

The verdict of the ISC's performance in the early years of its formation has been somewhat mixed. Some have criticised the committee for "resting too comfortably in the warm embrace of the Whitehall village".[47] At the same time, the ISC was having to design an effective culture of oversight when none to speak of had existed before, and when there were very few clues in the ISA as to how it should be done.[48] In the eyes of Peter Gill of Leicester University at least, the ISC had in its early years somewhat "exceeded … expectations".[49] It had taken on for itself some degree of operational scrutiny, even though this was not technically part of its mandate until the Justice and Security Act of 2013,[50] and had produced some reasonably probing reports into such issues as the Mitrokhin affair,[a] the intelligence concerning Iraqi weapons of mass destruction, and the treatment of detainees at Guantanamo Bay.

In the post-Snowden environment, the verdict on the ISC could be said to be similarly mixed. It is the case that the ISC undertook immediate action to investigate allegations of illegality on the specific question of the PRISM programme following Edward Snowden's revelations in 2013 (eventually ruling in favour of the government).[b] The subsequent breadth of the Privacy and Security Inquiry, which published its findings two years later, undoubtedly provided one of the most significant inputs to the drafting of the new IPA bill, and its inquiry reports into Detainee Mistreatment and Rendition could hardly be said to have pulled any punches.

In other ways, however, the ISC (much like its counterparts in other countries) is almost inevitably somewhat toothless, with a mandate to complain when things go wrong but no power to see any action necessarily result. The ISC noted in its report on the UK-authorised drone strikes in Syria in September 2015, for example, that the failure by the government to make available to its inquiry a number of sensitive documents had been "profoundly disappointing" and "had a significant bearing on the conclusions".[51] More pertinently, when the IPT ruled that data sharing arrangements between GCHQ and NSA under the latter's PRISM programme were insufficient to protect human rights between 2007 and 2014, when new guidelines were drafted,[52] doubts inevitably persist in some quarters that the ISC is either unwilling to censure the security services, or has insufficient access to information within the agencies it is supposed to be overseeing.[53]

Most of Edward Snowden's revelations focused on the question of bulk interception and electronic surveillance, and particularly on the extraordinarily intertwined Sigint relationship between the National Security Agency (NSA) in the US, and GCHQ in the UK.

[a] The Mitrokhin Inquiry looked into concerns that arose following the defection to the UK in 1992 of the KGB archivist, Vassili Mitrokhin, and the subsequent publishing of two books based on his smuggled archival material by the MI5 official historian, Christopher Andrew. The ISC-led inquiry was critical of MI6 on a number of counts concerning excessive secrecy, and a failure to bring forward for prosecution a number of known spies, notably Melita Norwood.

[b] PRISM is a US system for intercepting and databasing the content of communications passing through major social media networks based in the US. As the UK's GCHQ has reciprocal access to such data, an allegation had arisen that the UK was circumventing UK law by using data collected by its American partner.

Inquiry's findings

- Two cases where British intelligence officers appeared to have been directly involved in the mistreatment of detainees.
- 13 other cases where mistreatment was witnessed by British intelligence officers.
- 128 cases where foreign intelligence partners spoke about the mistreatment of detainees.
- 232 documented cases where intelligence was shared with partners known to regularly practice mistreatment, and 198 cases where intelligence was received from such partners.
- Two instances of British intelligence agencies offering to pay for the extraordinary rendition of suspects; and 22 cases where British intelligence directly led to the illegal rendition of suspects.
- At least one case, MI6 clearly turned a blind eye to mistreatment being used in the interrogation of a suspect by a third-party partner, and indeed fed questions in to the interrogation.
- Particularly in the defence intelligence realm, there was evidence that pooled intelligence shared with multiple partners almost certainly contained intelligence derived from mistreatment.
- Cases where some intelligence officers were not always fully aware of what did and did not constitute mistreatment, including in the hooding of detainees.
- There was evidence that GCHQ, which supplies intelligence derived from intercepted communications both to MI5 and MI6 and to selected foreign intelligence partners but is not generally present "in-theatre", considers itself to be somewhat "one step removed" and generally happy to rely on broad assurances that standards are being upheld.
- Evidence that British intelligence officers must have "known or reasonably suspected" that key al-Qaida suspect, Khalid Sheikh Mohammed, among others, were subjected to shocking amounts of waterboarding.
- That "general assurances" that the US would uphold the same level of human rights compliance as the UK were accepted in blanket fashion, despite mounting evidence to the contrary.
- British intelligence officers on the ground were either unwilling to raise questions about apparent mistreatment, or did so only half-heartedly, for fear that they would damage the overall intelligence relationship with the Americans.

As noted, consternation at the scale and volume of this exchange of digital data led to allegations that GCHQ were accessing intercepted material via their American partners in ways that would be illegal under UK law. To the ISC's credit, a swift and probing investigation was undertaken with GCHQ that found no evidence of illegal circumvention of surveillance law in this particular case.[54]

The Detainee Mistreatment and Rendition Inquiry

Aside from its investigations into bulk data sharing with the UK's key intelligence partners, one of the more significant investigations undertaken by the ISC in recent years has been that into the question of detainee mistreatment and rendition in the post-9/11 years. This investigation struck at the heart of intelligence relationships with the wider range of partners in the counter-terrorism realm outside of the Five-Eyes relationships; with many of whom serious questions concerning human rights abuse were hanging in the air.

For the UK, allegations that it may be complicit in serious abuse of terrorist suspects through its close intelligence relationship with the US began circulating very early after the announcement of the GWOT by President Bush. There were also serious concerns, formally expressed eventually by the Chilcot Inquiry, about the UK's involvement with the US in the invasion of Iraq in 2003 and the subsequent counter-insurgency. In 2008, the Gordon Brown government attempted to establish clearer and more transparent executive decision-making on major strategic national security issues with the creation of the National Security, International Relations and

Development Committee (NSIRD). This evolved subsequently into the National Security Council under the Coalition government in 2010.[55] It was at this stage that a full and formal inquiry was announced into the UK's involvement in the extraordinary rendition and mistreatment of terrorist suspects after 9/11.

Then British Prime Minister David Cameron claimed that he wanted to build public confidence in the inquiry's findings,[56] to which end he turned not to the ISC, but appointed the retired judge, Sir Peter Gibson, to head an independent inquiry called the Detainee Inquiry. Beset with legal complications concerning ongoing court cases, however, Gibson never completed the inquiry, and the whole process was handed over to the ISC in September 2014. This was eventually reported nearly four years later with two documents: one covering the initial period between 2001 and 2010; and the second considering the years thereafter.[57]

The process of conducting the inquiry was not without its complications and technically it remains unfinished at the time of reporting due to ongoing disagreements between the ISC and the government over the legal protection of witnesses.[58] This meant that junior officers active in MI5 and MI6 at the times in question could not be directly interviewed. Nevertheless, the inquiry did manage to take more than 50 hours of oral evidence and review approximately 40,000 classified documents, and its findings were significant. The chair of the ISC at the time of publication, Dominic Grieve QC, felt on balance that his committee had done its job to the best of its ability.[59]

The findings of the inquiry were broadly that there had been considerable problems for the UK in its relationship with the US in the early period (2001-2004), which did amount to complicity in the illegal rendition and torture of terrorist detainees, both by third parties and by the US itself.

From 2004 onwards, a slow realisation of the full extent of the US' use of EITs and "black sites" had led to a reappraisal of the intelligence relationship with the American agencies and the instituting of measures to lessen the risk, notably the publication of "consolidated guidance" for intelligence officers on how to appropriately deal with detainees. This has improved the situation, but there is still work to be done on ensuring abuses cannot happen again.

The problems were perhaps best summed-up by Craig Murray, a former British Ambassador to Uzbekistan in the early post-9/11 years when he said: "Were it not for me and my bloody-mindedness", noted Murray, "you would never know that these meetings had happened".[60] Murray relayed his exasperation to the ISC inquiry that numerous concerns he had raised about the use of torture in interrogations by the Uzbeks did not result in subsequent meetings being minuted properly, and thus the detail of such concerns could not be made available to the Foreign Affairs Select Committee on investigation.[61] The ISC concluded that the FCO was deliberately failing to commit such concerns to paper, lest it damaged the intelligence relationship with the Americans. The UK, it noted, saw itself as a "poor relation to the US".[62] This was clearly a considerable risk factor in the intelligence relationship with the US in the immediate post-9/11 years and led to the UK being complicit in illegal practices that contravened its general commitment to human rights.

After 2004

The year 2004 proved to be a turning point. Several reports started to emerge from human rights NGOs describing apparent abuses of detainees by US forces in Afghanistan and Iraq, and MI5 suspended interviews with British suspects in Guantanamo Bay following concerns about the conditions in which they were being kept.[63] Later that year, the infamous *60 Minutes* report was aired about the abuses

at the Abu Ghraib facility in Iraq, and the US publicly admitted for the first time their use of EITs on detainees.[64] This was followed in 2006 by an admission of the use of "black sites" to render and interrogate suspects in a legal limbo, by which time MI5 claims it was holding increasingly frequent internal discussions about the methods being used by the Americans and the potential reputational risk to be suffered in working with them.[65]

2004 also marked the beginning of a period in which MI6, MI5 and Defence Intelligence started issuing more detailed guidance to their officers about how to properly interview detainees in ways that complied with human rights obligations, including guidance on when and how to raise concerns. In 2009, then Prime Minister Gordon Brown announced that he had asked the ISC to establish a set of consolidated guidance for all intelligence officers, and this was duly published in 2010.

The Consolidated Guidance (CG) theoretically marked a watershed, after which the possibility of complicity in abuse conducted by intelligence partners is sharply reduced. The ISC admits that there has not yet been much reflection on whether the CG works in this aim, but compliance with it is monitored routinely by the Intelligence Services Commissioner (now subsumed within the IPCO) using a random sampling of cases.[66] Sir Mark Waller, the Commissioner for the period 2011-16, told the ISC that he was "broadly happy" that the various intelligence services were selecting the right cases to which the CG should apply, and were properly flagging up the cases in which there could be problems.[67]

Ongoing risks

It is important to note, however, that the CG should not be viewed as a panacea. Firstly, there is some debate about which cases should be subjected to the CG process, and which are out of scope. This is a judgement-call made by the intelligence services themselves and does run the risk that cases in which abuse may be suspected are not put through the process. Such cases would then never come to light unless a specific complaint was raised. As discussed, a particularly indicative case in this respect was that of the relationship with the Kenyans and their dealings with Michael Adebolajo. MI6 have continued to disagree with the ISC that the CG – that is, a consideration that this case could have involved effective complicity in mistreatment – is applicable to this case, and that it was rather a consular matter.[68]

This highlights a structural flaw in the CG and related considerations, which the current chair of the ISC emphasises is an important ongoing element of risk.[69] This is the question of intelligence relationships with joint units and the increased risk inherent in such relationships that abuse may be less visible and "lost in the noise". The ISC, and

Reprieve protestors (image credit: Val Kerry/ Flickr, 2008).

Sir Mark Waller, have flagged a specific concern that the CG does not adequately address the broader context of intelligence relationships with joint units, but only case-specific incidents and exchanges.[70] The issues are: if the UK is engaged with establishing a relationship with a joint intelligence unit overseas and with providing training and capacity-building for them, should they be permanently responsible for the overall level of conduct of all participants in the joint unit, or should such instances be investigated on a case-by-case basis as and when they come to light? The question is partly one of resources and capabilities, since perpetual monitoring of day-to-day conduct in an overseas joint unit is difficult, resource-intensive, and could be perceived as indicative of a fundamental lack of trust in the partner.

In some respects, this relates to the wider question of the utility and risks of capacity-building programmes in the modern era. As Jack Watling and Namir Shabibi noted, in a report for the Oxford Research Group, in the context of Yemen, such programmes involving multiple partners can be complex, politically fraught, cost-intensive and difficult to bring to a stage where they improve the situation rather than exacerbate existing problems and tensions both in terms of abuses and the UK's strategic influence. This is not to say that they are always redundant however: the right programme, properly managed, can deliver important dividends.[71]

From an intelligence point of view, the problems highlight the inherent element of consequentialism and cost-benefit appraisal that characterise calculations about whether to exchange intelligence with a partner, and whether this can be done in ways that allow hands to be kept clean.

Is oversight working?

In practical terms, the work embodied in the CG remains a work-in-progress. A draft revision of the CG extends its coverage beyond the three-state intelligence and security agencies, UK Armed Forces and Ministry of Defence (MoD) staff, to encompass the police intelligence community (the National Crime Agency and the Counter-Terrorism Command, SO15). Such an extension of the range of actors involved in intelligence sharing relationships on the ground seems entirely sensible.

In terms of oversight, the UK's ISC feels itself to be fairly robust in its ability to scrutinise the workings of key intelligence sharing relationships. In the eyes of the current ISC chair, both the parliamentary committee and the Investigatory Powers Commissioner's Office (IPCO) do have the remit to look at such relationships and do so "all the time".[72] This includes occasional visits abroad to discuss aspects of such relationships directly.

At the same time, however, the current chair of the committee does see fairly serious shortcomings in the lack of administrative resources available to it, especially when compared to counterparts such as the Senate parliamentary oversight committee in the US, for example, where every Senator has his or her own dedicated personal assistant. In the UK, the lack of staff means that the ISC can only really tackle one major and possibly one minor investigation at any one time, especially when other pressing political issues such as Brexit are in full flood and taking the time of the chair and his members.[73]

This does raise the risk that not every one of the manifold intelligence relationships in place can possibly be scrutinised by the Committee in normal times, and they will only be able to respond when specific problems or issues come to light. The IPCO, on the other hand, is better resourced, with around 70 staff at its disposal. This includes not only the 15 Judicial Commissioners who double-sign interception warrants, but approximately 50 staff with varying expertise (including technicians and lawyers), and the facility to call upon a Technical Advisory Panel where a specific technical issue needs to be tackled.[74]

Compared to many states, these figures represent a reasonably robust degree of oversight capability, although it is difficult to ascertain whether this number of staff is enough, since most of the detail of the investigations and scrutiny remain secret. The best indications are the annual reports of the Commissioner, which do give a broad-brush view of whether oversight seems to be proceeding satisfactorily. The last annual report in 2016 by the former Intelligence Services Commissioner,[c] Sir Mark Waller was robust in its praise for the general culture of legality and compliance in the intelligence services:

> *The UK Intelligence Community's attitude to ethics in general, and legal compliance specifically, is impressive and reassuring. While there is some legal debate about certain powers, I have never seen any evidence that the agencies institutionally would knowingly break the law. The application of the range of relevant legislation in this area is complex, and courts do not always agree with the position taken by the Government (or indeed by Intelligence Services Commissioners in the interpretations of the law we apply to our oversight). This does not mean they have not shown respect for the law.* [75]

Civil rights organisations remain circumspect, however, about whether the inherently covert nature of intelligence relationships means that they can ever be scrutinised fully and effectively. Privacy International, for example, suggest that intelligence sharing "is one of the most pervasive, and least regulated, surveillance practices in the modern world".[76] They further suggest that most intelligence sharing relationships "violate the principle of legality" since most are secret and are governed by non-existent legal statutes in the majority of cases. In the UK, for example, it is the case that surveillance law does not explicitly cover intelligence relationships per se. Such relationships can be scrutinised either in the context of "interference with property and wireless telegraphy outside of the UK";[77] of Covert Human Intelligence Sources and agents overseas;[78] or in relation to the aforementioned CG.[79] In practical terms, this generally means that scrutiny will focus either on partnership issues relating to bulk interception (and particularly on the relationship with the US); or on specific cases and issues to do with human intelligence exchanges, primarily in the counter-terrorism realm.

… the next best situation … is to ensure that there is a strong culture of legal awareness and compliance across all intelligence agencies, and that training and support of all officers is robust, effective, and constantly updated.

It is also the case that much of the scrutiny in the realm of the sharing of bulk communications data and related Sigint activities, not only in the UK across a range of European countries such as Italy, Germany, Sweden and the Netherlands, was triggered only by Edward Snowden's decision to leak a range of classified documents in 2013. It is also the case that the terrible episode of complicity in the torture of Abdel Hakim Belhaj at the hands of the Libyans, only came to light when the Gadhafi regime collapsed following NATO action and several classified documents were removed from government offices.[80] Subsequent investigations may have been thorough and delivered some degree of assurance and accountability in certain respects, but it does appear that most oversight and accountability over the pitfalls of intelligence relationships happens

[c] Since the passing of the Investigatory Powers Act in November 2016, the commissioner's role is subsumed within that of the new IPCO. This has not yet published an annual report at the time of writing.

rather reactively when specific cases slip out of the ring of secrecy.

Of course, many of these problems are not confined to the UK, and every state struggles with striking the right balance between the effective protection of key intelligence capabilities, and the effective oversight of such activities. The Detainee Mistreatment and Rendition Inquiry has uncovered that serious problems were generated by the UK's close intelligence relationship with the US and its wider counter-terrorism partners in the immediate years after 9/11, which amounted to complicity in widespread illegality under international human rights law. These are serious findings and they pose serious questions that must be answered fully by the government. At the same time, the inquiry also found that steps have been taken subsequently which have materially reduced the chance of such abuses happening in the future. The system is not perfect by any means – the CG, for example, should be subject to much further development – but matters could be said to be moving in the right direction.

Ultimately, if specific operations and relationships cannot be subjected to routine scrutiny, then the next best situation that can be achieved is to ensure that there is a strong *culture* of legal awareness and compliance across all intelligence agencies, and that training and support of all officers is robust, effective, and constantly updated in the pursuit of that aim. The words of the former Intelligence Services Commissioner that the legal and ethical culture in the UK's intelligence services is "impressive and reassuring" should not be taken lightly in this respect. [81]

Conclusions

In a globalised world with mounting transnational threats, typified by increasingly well-organised criminal and extremist movements and organisations, the imperative to share intelligence across boundaries is inescapable. Indeed, the UNSC has reminded all states that they have a responsibility to deliver the basic human right of security to all citizens, and part of this responsibility involves collectively maximising information advantages against adversaries.

If such an imperative needed underlining, the 9/11 attacks did this resolutely. For the US, the post-9/11 world was a new one in which a significantly broadened and deepened set of relationships with intelligence partners across the world became the new order of the day. Many of these partners included states with poor human rights records, but such considerations proved to be lower in priority than the need to establish effective intelligence sharing relationships in most cases.

There was a sense at the time that the new threat posed by the likes of al-Qaida was existential, in that unpredictable attacks, mass casualties, and a fear that terrorists would be willing to use chemical, biological or even nuclear devices, were changing the national security landscape beyond recognition. Scholars began to describe a "new terrorism"[d] of unprecedented threat; the UK Prime Minister at the time of the 9/11 attacks, Tony Blair, spoke of a shift in the "calculus of risk".[82]

For the UK and many other states, especially those in the West considered to be al-Qaida's "far enemy", the intelligence calculation was not only that staunch

[d] The phrase actually began circulating in the late 1990s following analysis of extremist movements such as Aum Shinrikyo in Japan and can probably be credited to Walter Laqueur: see Walter Laqueur, The New Terrorism: Fanaticism and the Arms of Mass Destruction. Oxford: Oxford University Press (1999), p.58.

solidarity should be shown to the Americans, but also that there was a direct and real fear that the next attack could be in their own countries. Many Western states were therefore happy both to expand their own intelligence relationships and to work closely with the Americans in so doing.

In this way, for a partner state such as the UK, a situation of double jeopardy was created. Firstly, when assumptions that the US would maintain the same legal standards as its other Western partners proved incorrect, the gathering realisation that new abuses were being committed by the Americans was somewhat put to one side, because of the importance of remaining a close partner to the Americans and their considerable intelligence capability. Secondly, the UK itself became complicit in abuses, sometimes directly and sometimes merely through association or the turning of a blind eye. In this way, some of the intelligence activity at the time did not alleviate the threat but arguably made it worse by radicalising a new generation of extremists.

Threats to human rights through intelligence sharing are realised when partner countries use received intelligence to carry out repressive and illegal actions, whether these be extra-judicial killings or arrests, illegal renditions, the torturing of detainees or indiscriminate military action. With increasingly voluminous and automated exchanges of intelligence data, especially in the realm of bulk interception of global communications, the risk of obfuscation of the audit trail between a single item of intelligence and an abuse being committed becomes ever greater.

A related risk, especially with "big data" exchanges, is that the ability of intelligence services to be able to assure the protection of universal rights to privacy and to apply the provisions of proportionality and necessity, becomes severely degraded. Furthermore, there is also a potential risk of the "outsourcing" of surveillance activities to partners in order to circumvent restrictive domestic laws.

The problem with intelligence sharing relationships, however, is that they are particularly sensitive elements of a state's covert activity, which, by definition, run heightened risks of compromise or manipulation. For these reasons, intelligence agencies will usually be at pains to keep relationships under wraps, often from their own oversight officials as much as from anyone else.

Very few states explicitly include intelligence relationships within the law and protocols governing the activities of their intelligence services, and it is usually similarly unclear whether and how oversight bodies and officials can scrutinise the nature of those relationships, other than in a reactive sense following the occurrence of a particular complaint or incident. This is not to say that intelligence relationships never come under detailed scrutiny – it appears in the case of the UK, for example, that they can and do – although this has to happen within the overall remit of operational scrutiny, which usually means a focus on particular selected operations rather than through a blanket process of scrutiny.

In the case of the UK, it is now clear that complicity in serious breaches of human rights was committed in the immediate years after 9/11, through the UK's close intelligence relationship with the US. This places the UK government's claims to be committed to upholding a "rules-based system" in its foreign policy and national security on somewhat flimsy foundations.

At the same time, there are some positive signs that progress towards learning from such mistakes is being made. The CG on detainee treatment, launched in 2010, is very significant, and must be further developed and evolved to ensure maximum protection against abuses. There are some complex questions to be asked about whether and how the day-to-day workings of

intelligence relationships should come under the scrutiny of the CG process, and there are also some specific and highly important questions to be answered about how to ensure the protection of human rights when those relationships are with joint, multi-agency intelligence units. These remain unanswered so far but are firmly on the agenda.

The ISC, despite its lacking resources and inability to go much beyond embarrassing the executive where warranted, has undertaken some excellent and unflinching analysis about pitfalls and misdeeds in intelligence activity, and it must continue to hone and develop its ability and impulse to do so. It should be ably assisted in this work by the new and reconfigured IPCO body.

On the bulk data front, complex and probing investigations have been undertaken following Edward Snowden's revelations, and these have not yet found any concrete evidence of illegal "outsourcing". Investigations have found sometimes lacking or withheld information about procedures and safeguards, and these are being addressed when found. The question of protecting the universal right to privacy in a world of massive-scale bulk communications data sharing is a much more difficult one to resolve, and the UK will be mindful that it recently lost a long-running battle with the High Court and the European Court of Justice over the provision of appropriate protections within the new IPA bill.[83]

The feeling of civil rights organisations such as HRW and Amnesty is that diplomatic assurances that received intelligence will not lead to abuses, are largely worthless in many cases. Their response is an absolutist one, namely that relationships with countries who cannot be trusted to comply with human rights cannot be tolerated and have to cease. For national security agencies operating in a complex world of interests and relationships, such a zero-sum position is probably untenable, and could itself be accused of failing to ensure human rights by denying key intelligence to law enforcement bodies.

For the foreseeable future, therefore, intelligence sharing and intelligence relationships will remain a staple part of the diet of contemporary warfare and security. This is not to say that serious risks are not continually present, as the post-9/11 period showed in highly problematic ways. The challenge is to continually evolve and develop the operational guidance and oversight such that the risk of major problems occurring is increasingly reduced.

Endnotes

[1] Shashank Joshi, 'Future Wars Will Need a More Versatile Response' (13 July 2015), retrieved on September 15, 2017, from http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11735180/Future-wars-will-need-a-more-versatile-response.html; Economist 'Missing in Action' (8 March 2014), retrieved November 15, 2017, from http://www.economist.com/news/britain/21598654-britain-needs-strategy-make-best-use-its-shrinking-military-capabilities-it-isnt.

[2] Emily Knowles and Abigail Watson, "All Quiet On The ISIS Front: British Secret Warfare In The Information Age" (March 2017), retrieved September 15, 2017, from https://www.oxfordresearchgroup.org.uk/all-quiet-on-the-isis-front-british-secret-warfare-in-an-information-age.

[3] UN Security Council, 'Resolution 2396' (21 December 2017) from: https://digitallibrary.un.org/record/1327675/files/S_RES_2396%282017%29-EN.pdf, p.3

[4] HMG, "Fact Sheet 1: Our Approach to the National Security Strategy". https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62483/Factsheet1-Our-Approach-National-Security-Strategy.pdf.

[5] Cited in Pakistan Institute of Legislative Development and Transparency (2007*) Peace and Conflict in Pakistan: The Structure and Role of Intelligence Agencies*. Islamabad, PILDAT, Dialogue Group on Civil-Military Relations, Background Paper, August 2007, p.9.

[6] Cited in Richard P. Mitchell, *The Society of the Muslim Brothers*. New York: Oxford University Press (1969), p.27.

[7] Frank Foley, *Countering Terrorism in Britain and France: Institutions, Norms and the Shadow of the Past*. Cambridge: Cambridge University Press (2013), p.248.

[8] Martin Rudner, "Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism". International Journal of Intelligence and Counterintelligence 17:2 (2004), p.214.

[9] Elizabeth Sepper, "Democracy, Human Rights, and Intelligence Sharing". *Texas International Law Journal* 46 (2010), p.175.

[10] Ephraim Kahana, "Mossad-CIA Cooperation". *International Journal of Intelligence and Counterintelligence* 14:3 (2001), p.414.

[11] http://www.middleeasteye.net/columns/raw-truth-about-uk-israel-special-relations-456740882.

[12] Lauren Gambino, "Yemen war: senators push to end US support of Saudi Arabia". The Guardian (28 February 2018). https://www.theguardian.com/world/2018/feb/28/yemen-saudi-arabia-war-us-support-senator-push-to-end.

[13] Emily Knowles, "We Need to Talk about Yemen," *Remote Control Project* (blog), December 9, 2016, https://www.oxfordresearchgroup.org.uk/Handlers/Download.ashx?IDMF=d8ca7ac6-d32b-4d71-b7b9-1233b3288a6f.

[14] Richard Norton-Taylor, "UK special forces and MI6 involved in Yemen bombing, report reveals". The Guardian (11 April 2016). https://www.theguardian.com/news/defence-and-security-blog/2016/apr/11/uk-special-forces-and-mi6-involved-in-yemen-bombing-report-reveals.

[15] Amnesty International, *Deadly Assistance: The role of European states in US drone strikes.* London: Amnesty International (2018), p.2.

[16] HM Government, *National Security Capability Review*. London (March 2018). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf, p.7.

[17] Foreign and Commonwealth Office (FCO), "UK government reaffirms its commitment to combat torture" (26 June 2017). https://www.gov.uk/government/news/uk-government-reaffirms-its-commitment-to-combat-torture.
[18] See UNGA, "Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment" (26 June 1987), Article 7, at https://www.ohchr.org/Documents/ProfessionalInterest/cat.pdf.
[19] Michael Walzer, "Political Action: The Problem of Dirty Hands", *Philosophy and Public Affairs* 2:2 (Winter 1973), p.161.
[20] Derek S. Reveron, "Old Allies, New Friends: Intelligence-Sharing in the War on Terror", *Orbis* (Summer 2006), p.458.
[21] Julian Richards, "Intelligence, Count-Insurgency and Reconstruction: Intelligence and International Cooperation in Afghanistan*".* Inteligencia y seguridad 13 (2013), pp.177-8.
[22] Daniel Carey, "Maya Evans case: secret courts, torture and avoiding embarassment". The Guardian (11 January 2013). https://www.theguardian.com/law/2013/jan/11/maya-evans-secret-courts-torture.
[23] Intelligence and Security Committee (ISC), *Detainee Mistreatment and Rendition, 2001-10*. London: TSO, HC1113, p.123-4 [hereafter: ISC DMR 2001-10].
[24] Ibid.
[25] BBC News, "Compensation to Guantanamo detainees 'was necessary'" (16 November 2010). https://www.bbc.co.uk/news/uk-11769509.
[26] Will Hutton, "In the Belhaj case, Britain set aside the rule of law and moral principles". The Guardian (13 May 2018). https://www.theguardian.com/commentisfree/2018/may/13/in-case-of-belhaj-britain-set-aside-rule-of-law-and-moral-principles.
[27] Cited in Hutton, "In the Belhaj case".
[28] See Amnesty International's report: "Morocco: Endemic torture used to incriminate suspects, gag dissent" (19 May 2015): https://www.amnesty.org/en/latest/news/2015/05/morocco-endemic-torture/.
[29] Intelligence and Security Committee (ISC), *Report on the intelligence relating to the murder of Fusilier Lee Rigby*, London: TSO, HC 795 (25 November 2014), p.153 [Hereafter: ISC, *Lee Rigby*].
[30] ISC, *Lee Rigby*, p.155.
[31] ISC, *Lee Rigby*, p.157.
[32] ISC, *Lee Rigby*, p.157.
[33] Interview with author, 16 July 2018.
[34] See: Ryan Gallagher, "How secret partners expand NSA's surveillance dragnet". The Intercept (19 June 2014). https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/.
[35] Gallagher, "How secret partners".
[36] Privacy International, *Secret Global Surveillance Networks: Intelligence Sharing between Governments and the Need for Safeguards*. London: Privacy International (April 2018), p.10.
[37] Privacy International, *Secret Global Surveillance Networks*, p.24.
[38] See the ISC's press statement; "Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme" (17 July 2013), on the ISC website at: http://isc.independent.gov.uk/news-archive?offset=40 .
[39] ISC press statement, "PRISM".
[40] See: Harriet Agerholm, ""UK mass surveillance programme violates human rights, European court rules". The Independent (13 September 2018). (https://www.independent.co.uk/news/uk/politics/uk-mass-surveillance-gchq-eu-human-rights-echr-edward-snowden-a8535571.html.
[41] Amnesty International, *Deadly Assistance*.

[42] See for example: German-Foreign-Policy.com, "Proposed for killing" (1 June 2015). https://www.german-foreign-policy.com/en/news/detail/6518/.
[43] Amnesty International, *Deadly Assistance*, p.7.
[44] Amnesty International, *Deadly Assistance*, p.7.
[45] *Die Gesetzes zur Ausland-Ausland Fernmeldeaufklärung des Bundenachtrichtendienstes* (Laws on Foreign-to-Foreign Intelligence Gathering of the Federal Intelligence Service).
[46] Thorsten Wetzling, "Germany's intelligence reform: More surveillance, modest restraints and inefficient controls", *Stiftung Neue Verantwortung*, Policy Brief (June 2017), p.3.
[47] Peter Gill, "Evaluating intelligence oversight committees: The UK Intelligence and Security Committee and the 'war on terror'", *Intelligence and National Security* 22:1 (2007), p.31.
[48] Mark Phythian, "The British experience with intelligence accountability", *Intelligence and National Security* 22:1 (2007), p.97.
[49] Gill, "Evaluating intelligence oversight committees", p.32.
[50] Prior to 2013, the ISC was technically only responsible for "functional oversight", namely checking that there has been proper compliance with processes, but not being able to scrutinise particular operations. In practice, however, it did undertake a degree of operational investigation before that time, albeit post facto.
[51] Intelligence and Security Committee (ISC), *UK Lethal Drone Strikes in Syria*, London: TSO, HC 1152 (26 April 2017), p.3..
[52] Owen Bowcott, "UK-US surveillance regime was unlawful 'for seven years'". The Guardian (6 February 2015). https://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa.
[53] Alan Travis, "ISC report acknowledges failings but paves way for snooper's charter". The Guardian (12 March 2015). https://www.theguardian.com/us-news/2015/mar/12/intelligence-agencies-finally-understand-need-to-step-out-of-the-shadows.
[54] See ISC press statement, "PRISM".
[55] Julian Richards, *A Guide to National Security*. Oxford: Oxford University Press (2012), p.21.
[56] Ian Cobain, "Why did the Gibson inquiry into rendition disappear?" The Guardian (6 July 2015). https://www.theguardian.com/commentisfree/2015/jul/06/gibson-inquiry-rendition-david-cameron-uk-torture.
[57] See ISC website at http://isc.independent.gov.uk/committee-reports/special-reports.
[58] ISC, *DMR 2001-10*, pp.9-10.
[59] Interview with the author, 16 July 2018.
[60] Ibid.
[61] ISC DMR 2001-10, p.60.
[62] Ibid.
[63] ISC *DMR 2001-10*, p.69.
[64] ISC *DMR 2001-10,* p.69.
[65] ISC *DMR 2001-10*, p.59.
[66] Intelligence and Security Committee (ISC), *Detainee Mistreatment and Rendition: Current Issues*, London: TSO, HC 1114, pp.1, 19-20 [Hereafter: ISC, *Current Issues*].
[67] ISC, *Current Issues*, p.22.
[68] ISC, *Current Issues*, p.51.
[69] Interview with author, 16 July 2018.
[70] ISC, *Current Issues*, p.50.
[71] See Jack Watling and Namir Shabibi, "British Training and Assistance Programmes in Yemen, 2004 – 2015". Oxford Research Group, Remote Warfare Programme, Briefing number 4 (June 2018).
[72] Interview with author, 16 July 2018.

[73] Interview with author, 16 July 2018.
[74] Investigatory Powers Commissioner's Office (IPCO). https://www.ipco.org.uk/
[75] The Rt Hon. Sir Mark Waller (Intelligence Services Commissioner), "Report of the Intelligence Services Commissioner for 2016", London (20 December 2017), p.5. https://www.ipco.org.uk/docs/Intelligence%20Services%20Commissioner%20Annual%20Report%202016.pdf.
[76] Privacy International, *Secret Global Surveillance*, p.3.
[77] To which ISA Section 7 applies, and primarily in the context of "bulk interception" of overseas communications.
[78] To which ISA Section 7 and the Regulatory and Investigatory Powers Act (RIPA) Part 2 apply.
[79] The CG has not yet been explicitly placed on the Statute Books within surveillance law, but is an established mechanism.
[80] Will Hutton, "In the Belhaj case".
[81] The Rt Hon. Sir Mark Waller, "Report of the Intelligence Services Commissioner"
[82] BBC News, "Blair terror speech in full", (5 March 2004). http://news.bbc.co.uk/1/hi/3536131.stm.
[83] Owen Bowcott, "EU's highest court delivers blow to UK snooper's charter", The Guardian (21 December 2016). https://www.theguardian.com/law/2016/dec/21/eus-highest-court-delivers-blow-to-uk-snoopers-charter.