Intelligence Sharing in Remote Warfare

https://www.e-ir.info/2021/02/17/intelligence-sharing-in-remote-warfare/

JULIAN RICHARDS, FEB 17 2021

This is an excerpt from *Remote Warfare: Interdisciplinary Perspectives*. Get your free download from E-International Relations.

In the post-9/11 period, the logic of remote warfare for Western powers has been greatly affected 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 undoubtedly increasing the lure. Coupled with these drivers, advancements in technology are encouraging Western nations to establish relationships and capabilities with partners that allow for intelligence collection from afar. These developments can offer security dividends if conducted effectively but can also come with a potential cost to state and society. This chapter examines the role that intelligence sharing plays in the broader concept of remote warfare and evaluates the likely risks to state and society. It considers the ways in which intelligence sharing underpins developments, in the shape of the sharing of bulk data at speed and the networking of weapons systems. In a sense, intelligence is the glue that binds together partners and agents in the whole development of the remote warfare landscape.

There are undoubtedly strong drivers to develop and enhance intelligence sharing relationships in the modern environment of conflict and risk (Aldrich 2004; Reveron 2006; Richards 2018), and these are evaluated here. Not all of these drivers are necessarily nefarious, and, if safeguards are observed, intelligence sharing has the potential to make the world a safer place. If done badly, however, the sharing of intelligence can run the risk of outsourcing 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 (Krishnan 2011). In the case of a country such as the UK, the more partners with whom intelligence is shared 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. A case study is then examined of the UK in the post-9/11 environment, and the challenges it has faced in its intelligence sharing activities.

A related danger concerns the 'bulk' sharing of intercepted material, as Edward Snowden revealed was happening between the US and multiple allies, including the UK, in his release of classified material in 2013. Here, the risk is that highly complex and integrated signals intelligence (Sigint) systems sharing ever more industrial-scale amounts of data, could allow for unverified misuse of intelligence. There is a risk to privacy here as much as a risk of abuse.

Added to these problems is the fact that a state's oversight of its intelligence agencies and their activities can be inherently difficult (Phythian 2007; Gill 2012; Dobson 2019). Within this landscape, intelligence sharing relationships are often among the most sensitive aspects of any intelligence agency's operations. Such relationships are usually shrouded in heavy secrecy, not only from the public but occasionally from a state's own oversight bodies. States will argue national security reasons for this needing to be so, but going forwards, the importance of due diligence and robust oversight of intelligence sharing relationships and operations will need to be highly developed if serious risks to state and society are not to be realised.

The case for intelligence sharing

In many ways, 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) passed Resolution 2396 in 2017, reminding member states of the need for 'timely information sharing, through appropriate channels and arrangements' to disrupt the planning of attacks (UNSC 2017, 3).

As the erstwhile Director-General of Britain's MI5 intelligence agency, Eliza Manningham-Buller, noted (ISC 2018a, 134), the 9/11 attacks marked a watershed following which 'the need for enhanced international cooperation to combat the threat from al-Qaida and its affiliates' was taken as a given. Such threats from international terrorism have become more dynamic, with new connections and lines of information being forged across the globe with increasing ease and rapidity.

In the intelligence world, the 'Five Eyes' relationship which flowed from shared experiences in the Second World War, encompasses highly integrated intelligence sharing between the US, UK, Canada, Australia and New Zealand. Intelligence sharing operates on several other levels, however, many of which are far less structured and avowed than the Five Eyes or NATO. In some cases, a collection of states will participate in semi-structured, multilateral fora for sharing intelligence – a good example being the Club of Berne's group of Western security agencies (Walsh 2006), whose membership closely mirrors that of NATO.[1] At the tactical level, particular agencies will also sometimes participate in multinational intelligence 'hubs' or 'fusion centres'[2], usually dealing with specific issues such as regional counter-crime or counterterrorism. Beneath all of these more formal relationships, a myriad of bilateral or multilateral intelligence relationships will operate between states, with very focused objectives and mechanisms.

In all cases, intelligence sharing is a particularly sensitive and secretive business. The lifeblood of any security agency is the set of covert sources and capabilities it is able to deploy in ways that garner strategic advantage over adversaries (Warner 2002). The loss or compromise of such capabilities can lead to instant operational failure, and often political ignominy. Like reputations, sensitive intelligence sources take a long time to establish, but can be destroyed very quickly. Forging a relationship with a partner can often be about a complex web of mutual interests, whereby information is just one of the standards of currency.

Geography is usually crucial in prompting a relationship. In a sense, this is a key catalyst for remote warfare, as national security threats migrate out to the badlands of Asia, Africa and the Middle East. Such considerations provide the rationale for capacity-building projects, through which investments can be made in the capability of local partners. In the Five Eyes context, the dispersed geography of the partners was useful in establishing global interception systems such as ECHELON (Perrone 2001). More recently, evidence suggests that a number of airbases in Europe provide crucial communications infrastructure for directing the US' remote targeting across the Middle East, North Africa and South Asia (Amnesty International 2018, 6).

Such relationships may be asymmetric in the sense that the state reaching out to establish the partnership may receive benefits in a different area in return. These might not even be about intelligence capabilities *per se*, but could encompass military aid or other economic investments. This also means that such relationships can work both ways and that threats can be made to 'turn off the tap' if there are political or diplomatic problems – as Pakistan, for example, has frequently suggested to the US (Bokhari et al 2018). In many ways, this mirrors the wider problem of perverse incentives created by long-term military aid programmes, of which intelligence capacity-building is often a part (Bapat 2011; Boutton 2014).

There is a particular factor here concerning terrorism. One of the key benefits is that counterterrorism (like counter-crime) tends to transcend all other political considerations, even if definitions of who the 'terrorist' is can vary considerably in the face of local political objectives. That aside, from a policy perspective, the basic strategic concept of countering transnational terrorism can be the one topic on which virtually every state agrees, even if they do not in most other aspects. This applies to Western relationships with Russia and China, for example, and to relationships with Middle Eastern states.

Difficulties and challenges

A key principle of intelligence sharing is the 'third-party rule', which means that any country receiving intelligence from a partner agrees not to share it onwards with another party – unless they have express permission to do so. This agreement relies on mutual trust and it is not always possible to be certain where a piece of intelligence has ended up. There is, of course, also the constant risk that a partner agency may be infiltrated or corrupted by a hostile power.

A number of recent inquiries into intelligence activity have established that intelligence sharing relationships with international partners are rarely the subject of formal and documented memoranda of understanding (MoUs). Indeed, agencies such as MI6 point out that such formal arrangements are usually avoided, not only in order to keep the details to the minimum, but also because a fundamental lack of trust can be implied if the UK always insists on everything being formally documented and bureaucratised (ISC 2018b, 62). For an agency whose business is establishing relationships with states outside of the West with a different culture of bureaucratic norms, such factors must be taken carefully into account. On the other hand, as a former Ambassador to Uzbekistan noted, not documenting joint intelligence activities can sometimes turn out to be for reasons of the concealment of abusive behaviours (ISC 2018a, 60).

'Diplomatic assurances' are the formal method whereby intelligence partners commit to safeguarding human rights, and these have been established with several partner countries in the post-9/11 period. But human rights organisations such as Human Rights Watch (HRW) are scathing about the utility of such instruments as a safeguard against abuse (HRW 2005, 3). Amnesty International has echoed their sentiments, noting that 'the best way to prevent torture is to refuse to send people to places where they risk being harmed' (cited in Richards 2013, 183).[3]

It is the case that most non-Western states do not have clearly delineated and articulated expressions of their national security objectives and strategy (see for example HMG n.d.). In many cases, national security is just what a state must do to protect itself. 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.

The founder of the Muslim Brotherhood in Egypt, Hassan Al-Banna, was right in his prediction that entrenched states in the Middle East would always wish to repress populist Islamist movements (Mitchell 1993, 30). Western countries generally share this objective, and this drives much contemporary intelligence sharing. But the problem is that the underlying conception of national security may be different between states, and sometimes dangerously so. The problem can often manifest itself in the partner country wishing to obtain intelligence on expatriate dissident movements rather than on 'terrorists' per se, as a quid pro quo for supplying intelligence on terrorist suspects. For the UK, where London has been lambasted in the past as a haven for radicals and dissidents (Foley 2013, 248), this can be an attractive element for countries that wish to obtain intelligence on London-based political oppositionists. Rudner (2004, 214) describes how Egypt and Jordan have both complained to the UK about its failure to supply them with intelligence on dissidents residing in London, while Sepper (2010, 175) describes the case of the Libyan authorities being able to interrogate detainees at Guantanamo Bay about dissidents in the UK.

Conversely, intelligence provided to such countries on purported terrorist targets can lead to violent actions being taken on the ground, violating human rights, neutralising potential further sources of intelligence, and generating political blowback. After 1981, the US allegedly slowed the flow of intelligence to Mossad after the Israelis had used their information to destroy Iraq's nascent nuclear reactor in a pre-emptive military strike (Kahana 2001, 414). More recently, heavy military actions against Hamas and Hezbollah within the Occupied Territories continue to place Western military and intelligence partners of Israel in uncomfortable positions concerning complicity with disproportionate military action in civilian areas (Curtis 2018).

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 bombings that have caused considerable

civilian casualties (Gambino 2018), not to mention a humanitarian catastrophe affecting much of the population. 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 (Norton-Taylor 2016). Such operations are framed by the states in question as tackling 'upstream' terrorist threats from the likes of al-Qaeda in the Arabian Peninsula (AQAP). But the question has to be asked – to what cost?

Case study: the UK's post 9/11 security environment

Officially, the UK makes a great deal of its mission to uphold values in its foreign policy. On the occasion of the 2017 International Day in Support of Victims of Torture, the Foreign and Commonwealth Office's (FCO) Minister for Human Rights, Lord Ahmad, noted that 'The UK government condemns torture in all circumstances' (FCO 2017). Urging other states to 'sign, ratify and implement' the UN Convention Against Torture and its Optional Protocol can feel disingenuous, however, when the UK itself becomes embroiled in detainee mistreatment scandals or arms sales to repressive regimes.

In Afghanistan in the post-9/11 period, operational collaboration with the new intelligence agency, the National Directorate of Security (NDS), has proved to be a complicated business. In 2007, Amnesty International revealed a catalogue of human rights abuses in Afghanistan and ISAF's alleged complicity in the abuse, much of it centred around the NDS's notorious 'Department 17' facility in Kabul (Richards 2013, 177–8). In 2012, the British peace activist Maya Evans was successful in securing a judicial review that placed a temporary moratorium on detainee handovers in Afghanistan (Carey 2013).

One of the more significant individual cases in the post-9/11 period was that 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 subsequently mistreated over a period of three months (ISC 2018a, 123–4). He alleged he was then illegally rendered to Morocco and thereafter to Guantanamo Bay, where he was subjected to further mistreatment (ISC 2018a, 124). In 2010, the UK 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, for undisclosed sums believed to number in the tens of millions of pounds (BBC News 2010).

The case of a Libyan dissident opposed to Muammar Gaddafi by the name of Abdel Hakim Belhaj caused similar political controversy. Belhaj was illegally rendered from Thailand to Libya by the CIA in 2004, acting on British intelligence (Hutton 2018). Allegations of subsequent brutal torture by the Libyans culminated in a claim against the British government for £1 in compensation and a full apology, eventually settled in May 2018, when a statement was delivered to parliament on behalf of the Prime Minister, apologising 'unreservedly' and lamenting Belhaj's 'appalling treatment' (Hutton 2018).

In both cases, the defining features were a willingness by UK intelligence agencies to work with unsatisfactory regimes to pursue their counter-terrorism objectives; and complicity in the mistreatment of detainees through a desire not to disrupt the key intelligence relationship with the US

Meanwhile, one of the perpetrators of the 2013 murder of Fusilier Lee Rigby, Michael Adebolajo, has alleged that he was beaten and threatened with electrocution and rape on more than one occasion during detention in Kenya at the hands of a police unit with a relationship with British intelligence (ISC 2014, 153). Leaving aside his subsequent conviction for murder, the allegations highlighted a number of 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. One major area of risk highlighted by the case was the question of which intelligence has been potentially derived from torture where multiple agencies were working together, and where intelligence is pooled in such a way that the provenance of individual pieces of information may be difficult to ascertain. The Chair of the Intelligence and Security Committee (ISC) has identified this as a significant area of ongoing risk.[4]

One of the more noteworthy investigations undertaken by the ISC in recent years has been that into the question of

the mistreatment and rendition of detainees in the post-9/11 years (the Detainee Mistreatment and Rendition [DMR] Inquiry). This investigation struck at the heart of intelligence relationships with the UK's range of partners in the counterterrorism realm, with many of whom serious questions concerning human rights abuses were hanging in the air.

The problems in the early period after 9/11 were manifold. In all, the Inquiry found two cases where British intelligence officers appeared to have been directly involved in the mistreatment of detainees. There were 13 other cases where mistreatment was witnessed by British intelligence officers, and 128 cases where foreign intelligence partners spoke about the mistreatment of detainees. There were 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 were found 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.

The details amount to a comprehensive realisation during this period of the risk that intelligence relationships can lead to the serious compromise of human rights. Aside from some cases of apparent direct complicity in mistreatment, there was clear evidence of a lack of training amongst intelligence officers about what does or does not constitute mistreatment (ISC 2018a, 131). There was also evidence that parts of the British intelligence machinery either had no mechanism for filtering out intelligence that may have been derived from torture, or were generally happy to rely on broad assurances that standards were being upheld, when they should have had strong grounds for suspecting otherwise (Ibid., 55). On the key intelligence relationship with the Americans, the DMR Inquiry found evidence that 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 (Ibid., 58). This constituted a serious structural risk in the system.

From 2004 onwards, the DMR Inquiry found evidence of the situation starting to change for the better. In 2010, the Consolidated Guidance (CG) on how to properly handle detainees was issued to all intelligence officers on the ground. Sir Mark Waller, the Intelligence Services Commissioner for the period 2011–16, subsequently 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 concerns (Ibid., 22).

The CG should not be viewed as a panacea, however. The ISC, and 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 (ISC 2018b, 50). 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 Watling and Shabibi (2018) noted 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 are adding value on the ground rather than exacerbating existing problems and tensions. This is not to say that they are always redundant, however: the right programme, properly managed, can deliver important dividends.

Risks to state and society

The discussion thus far has highlighted the potential dilemma for modern states engaged in remote warfare to balance the imperatives of sharing intelligence with partners to deliver national security, against the risk of 'dirty hands' (Walzer 1973, 161) that arises in doing so. The principal risk is that increased flows of intelligence between partners may mean safeguarding human rights not only becomes more difficult to ensure, but that even knowing where rights have been compromised will be increasingly difficult to establish.

For liberal democratic states such as the UK, the first and most obvious risk is a reputational one, whereby supposed commitments to universal human rights can start to sound like empty promises when cases of complicity in abuse arise. This could, in turn, reduce the influence of the UK on the world stage at a time when it can ill afford to do so.

For broader society, there are fundamental questions about a retrenchment from the core values of peace, democracy and human rights. In the intelligence sharing context, there are also public fears about an inexorable creep towards a global 'surveillance society' (Beck 2002; Kerr and Earle 2013; Lyon 2014; Richards 2016). At a time when authoritarian regimes are increasingly managing to place national security imperatives above commitments to modern liberal values, states such as the UK should be aiming to be the vanguard of such liberal values, rather than allowing themselves to fall into the same boat of authoritarianism, secrecy and abuse.

The advent of 'Big Data' (which means both a massively increased amount of available data on the activities of the citizenry; but also increasingly sophisticated technology for extracting value from such data) has delivered a complex set of opportunities and risks for the major intelligence services. On the partnerships front, 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. A secret National Security Agency (NSA) system uncovered by Snowden called RAMPART-A, for example, appears to be an international network of interception capabilities against trunk fibre-optic cables carrying the bulk of the global communications network (Gallagher 2014). The system is part of a network of 33 third-party Sigint relationships (Gallagher 2014).

Again, reputational issues concerning the conduct of liberal democratic states as opposed to those of authoritarian regimes such as China – who make no secret of the need to undertake near-ubiquitous surveillance of their citizenry – are placed on the table by such revelations.

As the civil rights NGO Privacy International (2018, 10) noted, there are three potential problems with these bulk surveillance activities. First is the question of the basic, extra-territorial human right to privacy. A related question is that of ensuring the legal protection against surveillance of the communications of a state's own nationals, and that of particularly sensitive interest-groups such as lawyers, doctors and journalists. Germany is one of the few countries that has taken steps to try to address this particular issue legislatively following a parliamentary inquiry[5], although in the view of one commentator, subsequent changes serve only to make oversight of the national intelligence service, the BND (Bundesnachrichtendienst*)*, even more confusing and fragmented (Wetzling 2017). In the UK, MI5 has recently been castigated for having 'lost control' of its data retention and handling in such a way that unlawful invasions of privacy may have become a systemic issue (Bowcott 2009).

In a case brought to the Investigatory Powers Tribunal by Privacy International against GCHQ in 2013 about access to an NSA system called PRISM (Privacy International 2018, 24), the parliamentary ISC committee found no evidence that GCHQ had been circumventing UK law through its access to the NSA system (ISC 2013). But, as with the abovementioned case against MI5's data handling, there may be a tendency amongst national intelligence services to conceal from their oversight bodies information that has not been explicitly requested. This could be either because something serious is amiss, or simply because adequate procedures have not been followed properly. Such cases undermine trust in the integrity of the agencies and in the capabilities of the state's oversight function.

Amnesty International (2018) 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 through the provision of geolocational data. 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, the revelation of the scale and complexity of data exchanges with the US on Somali piracy has triggered a comprehensive inquiry by the state's parliamentary oversight body, the CTIVD (Commissie van Toezicht op de Inlichtingen). 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 (Amnesty International 2018, 7).

The fundamental question here is perhaps a deep-rooted and significant one about the impact of new technology on society. As with the advent of artificial intelligence (AI) and automation, one can foresee both exciting new opportunities and grave risks, depending on one's point of view. For intelligence services, galloping technology in the areas of data collection, mining and analysis, offer tremendous new opportunities for tackling complex international threat actors and delivering national security. But there are also manifold risks in sliding towards authoritarianism and repression, and many of these are only just beginning to take shape.

Going forwards

The de-centred and borderless nature of contemporary threats such as those posed by al-Qaeda or Islamic State, means there is an increasingly inescapable logic in sharing intelligence with as many cooperative partners across boundaries as possible. Again, technological developments in database capacities, bulk data transmission and algorithmic analysis have encouraged and enabled such transformations.

The UK discovered to its cost after 9/11, however, that some intelligence relationships can, in the wrong circumstances, lead to complicity in serious human rights abuses. In many cases, these arose from the importance of the relationship with the US and the perceived need not to damage that relationship. But alliances with other partners across the world who see national security in very different ways to us can also lead to problems. As the volumes of data shared and the automation by which such sharing happens both scale up, the ability to track back from a specific piece of information to the delivery of a human rights abuse becomes ever more difficult to achieve. There are serious moral questions to be asked about allowing such concerns to drift, especially in supposedly liberal democratic states.

Placing all of this in perspective, the answer is probably not to bolt the stable door completely. The fundamental drivers for sharing intelligence across boundaries in the pursuit of organised crime and terrorism are inescapable and are indeed mandated by the UN to all responsible member states. As with so many areas of society, new technologies can deliver tremendous benefits in this area if they are used responsibly.

The UK and partner states need to learn from the mistakes of the immediate post-9/11 period and ensure as much oversight and accountability of their intelligence sharing relationships as they can deliver. It is recognised, of course, that sensitive technologies and relationships should not be trumpeted on the front pages of the newspapers, since that will just help the enemies of democratic society. At the same time, liberal democratic societies need to ensure that in all areas of the move towards remote warfare, the importance of protecting rights and ensuring accountability will remain paramount. Training and capacity-building of partners are not bad things and can indeed ensure that a rules-based and professional approach to security and intelligence becomes more widespread across states and society. Training and guidance for frontline officers working with partners also needs to be continually reviewed and developed.

In the rapidly developing area of data-sharing with partners, technology needs to ensure due diligence and audit functions for individual pieces of information as much as possible. To be fair, there is evidence that fears of outsourcing of illegal or unacceptable practices in this area have not been realised to any major extent, as far as can be determined. But the risks are rising continually as we move through the next major revolution in military affairs, and vigilance against eroding human rights needs to keep pace.

References

Aldrich, Richard J., 2004. 'Transatlantic Intelligence and Security Cooperation.' *International Affairs,* 80(4) (July): 731–53.

Amnesty International. 2018. *Deadly Assistance: The role of European states in US drone strikes.* London: Amnesty International.

BBC News. 2010. 'Compensation to Guantanamo detainees "was necessary".' 16 November. https://www.bbc.co.uk/news/uk-11769509

Beck, Ulrich. 2002. 'The Terrorist Threat: World Risk Society Revisited.' *Theory, Culture and Society,* 19(4): 39–55.

Bokhari, Fahran, Katrina Manson and Kiran Stacey. 2018. 'Pakistan halts intelligence sharing with US after aid suspension.' *Financial Times*. 11 January. https://www.ft.com/content/59969778-f6b1-11e7-88f7-5465a6ce1a00

Bowcott, Owen. 2019. 'MI5 accused of "extraordinary and persistent illegality."' *The Guardian*. 11 June. https://www.theguardian.com/uk-news/2019/jun/11/mi5-in-court-accused-of-extraordinary-and-persistent-illegality

Carey, Daniel. 2013. 'Maya Evans case: secret courts, torture and avoiding embarrassment.' *The Guardian*. 11 January. https://www.theguardian.com/law/2013/jan/11/maya-evans-secret-courts-torture

Curtis, Mark. 2018. 'The raw truth about the UK's special relationship with Israel.' *Middle East Eye*. 5 June. http://www.middleeasteye.net/columns/raw-truth-about-uk-israel-special-relations-456740882

Dobson, Melina J. 2019. 'The last forum of accountability? State secrecy, intelligence and freedom of information in the United Kingdom.' *The British Journal of Politics and International Relations,* 21(2: 3): 12–29.

FCO (Foreign and Commonwealth Office). 2017. 'UK government reaffirms its commitment to combat torture.' 26 June. https://www.gov.uk/government/news/uk-government-reaffirms-its-commitment-to-combat-torture

Foley, Frank. 2013. *Countering Terrorism in Britain and France: Institutions, Norms and the Shadow of the Past* . Cambridge: Cambridge University Press

Gallagher, Ryan. 2014. 'How secret partners expand NSA's surveillance dragnet.' *The Intercept.* 19 June. https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/

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

Gill, Peter. 2012. 'Intelligence, Threat, Risk, and the Challenge of Oversight.' *Intelligence and National Security,* 27(2): 206–22.

Hillebrand, Claudia. 2017. 'With or without you? The UK and information and intelligence sharing in the EU.'*Journal of Intelligence History,* 16(2): 91–94.

HMG. N.d. '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

HRW (Human Rights Watch). 2005. '*Still at risk: Diplomatic Assurances no Safeguard against Torture.'* 17/4(D). April.

Hutton, Will. 2018. 'In the Belhaj case, Britain set aside the rule of law and moral principles.' *The Guardian*. 13 May. https://www.theguardian.com/commentisfree/2018/may/13/in-case-of-belhaj-britain-set-aside-rule-of-law-and-moral-principles

Inkster, Nigel. 2016. 'Brexit, Intelligence and Terrorism.' *Survival,* 58(3): 23–30.

ISC (Intelligence and Security Committee). 2013. *Press statement*. https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20130717_ISC_statement_GCHQ.pdf

———. 2014. *Report on the intelligence relating to the murder of Fusilier Lee Rigby.* London: TSO, HC 795.

———. 2018a. *Detainee Mistreatment and Rendition Inquiry 2001-10*. London: TSO, HC113.

———. 2018b. *Detainee Mistreatment and Rendition: Current Issues*. London: TSO, HC 1114.

Kahana, Ephraim. 2001. 'Mossad-CIA Cooperation.' *International Journal of Intelligence and Counterintelligence,*

14(3): 409–20.

Kerr, Ian, and Jessica Earle. 2013 'Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy.' *Stanford Law Review Online*, 66/65.

Krishnan, Armin. 2011. 'The Future of US Intelligence Outsourcing.' *Brown Journal of World Affairs,* 18(1): 195–211.

Lyon, David. 2014. 'Surveillance, Snowden, and Big Data: Capacities, consequences, critique.' *Big Data and Society,* July–December.

Mitchell, Richard P., 1993. T*he Society of Muslim Brothers.* New York: Oxford University Press.

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

Perrone, Jane. 2001. 'The Echelon spy network.' *The Guardian*. 29 May. https://www.theguardian.com/world/2001/may/29/qanda.janeperrone

Phythian, Mark. 2007. 'The British experience with intelligence accountability.' *Intelligence and National Security,* 22(1): 75–99.

Privacy International. 2018. *Secret Global Surveillance Networks: Intelligence Sharing between Governments and the Need for Safeguards*. London: Privacy International. April.

Reveron, Derek S. 2006. 'Old Allies, New Friends: Intelligence sharing in the War on Terror.' *Orbis* (Summer 2006): 453–68.

Richards, Julian. 2013. 'Intelligence, Count-Insurgency and Reconstruction: Intelligence and International Cooperation in Afghanistan*.' Inteligencia y seguridad,* 13: 167–92.

Richards, Julian. 2016. 'Needles in Haystacks: Law, Capability, Ethics and Proportionality.' In*Big-Data Intelligence-Gathering,'* edited by Anno Bunnik, Anthony Cawley, Michael Mulqueen, and Andrej Zwitter. Basingstoke, Palgrave Macmillan.

Richards, Julian. 2018. *Defining Remote Warfare: Intelligence sharing after 9/11*. Remote Warfare Programme*,* Oxford Research Group.

Rudner, Martin. 2004. 'Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism.' *International Journal of Intelligence and Counterintelligence,* 17(2) 193–230.

Sepper, Elizabeth. 2010. 'Democracy, Human Rights, and Intelligence Sharing.' *Texas International Law Journal,* 46: 151–207.

UNSC (Security Council). 2017. 'Resolution 2396.' 21 December. https://digitallibrary.un.org/record/1327675/files/S_RES_2396%282017%29-EN.pdf

Walsh, James. I. 2006. 'Intelligence sharing in the European Union: Institutions are not Enough.'*Journal of Common Market Studies,* 44(3): 625–43.

Walzer, Michael. 1973. 'Political Action: The Problem of Dirty Hands.' *Philosophy and Public Affairs,* 2 (2) Winter: 160–80.

Warner. Michael. 2002. 'Wanted: A Definition of "Intelligence". Washington DC: Center for the Study of Intelligence. January: 15–22.

Watling, Jack. and Namir Shabibi. 2018. 'British Training and Assistance Programmes in Yemen 2004 –2015.' Remote Warfare Programme, Oxford Research Group. June.

Wetzling, Thorsten. 2017. 'Germany's intelligence reform: More surveillance, modest restraints and inefficient controls.' *Stiftung Neue Verantwortung*, Policy Brief. June.

Notes

[1] At the time of writing, the impact of Brexit on intelligence sharing relationships is unknown and subject to much conjecture (Inkster 2016; Hillebrand 2017).

[2] Examples include Interpol, Europol, CARICOM's Regional Intelligence Fusion Centre (RIFC) in the Caribbean region, or the Central Asia Regional Information and Coordination Centre (CARICC), to name but a few.

[3] Amnesty International, '*Europe must halt unreliable 'diplomatic assurances' that risk torture*http://www.amnesty.org/en/news-and-updates/report/europe-must-halt-unreliable-diplomatic-assurances-risk-torture-2010-04-12

[4] Interview with author, 16 July 2018.

[5] *Die Gesetzes zur Ausland-Ausland Fernmeldeaufklärung des Bundenachtrichtendienstes*; Laws on Foreign-to-Foreign Intelliegnce Gathering of the Federal Intelligence Service.

About the author:

Julian Richards has spent nearly twenty years working for the British Government in intelligence and security policy, before co-founding the Centre for Security and Intelligence Studies at the University of Buckingham where he is currently the Director. His research interests include intelligence machinery and governance; and counter-terrorism policy in a range of regional and global contexts.