6. Acting ethically in the shadows: Intelligence gathering and human rights

Richard Barrett and Tom Parker

At the outset, it is important to make a clear distinction between domestic and foreign intelligence collection. The techniques practiced in both disciplines are essentially the same, but there are nevertheless important, indeed critical, differences. In democratic societies, domestic intelligence collection is typically a well-regulated activity that takes place within the same broad legal framework as more traditional law enforcement activities. By contrast, foreign intelligence collection is often conducted with deliberate disregard for foreign laws, espionage is after all an inherently illegal activity, but it is not conducted in an entirely lawless manner. In democracies, externally-focused intelligence agencies operate in accordance with the domestic laws of their parent country, even when breaking other nations' laws overseas. International human rights law is every bit an obligation for the intelligence community as it is for any other field of government, although international law does recognize the legitimate sensitivities that surround issues relating to national security.

While recognizing the need for intelligence gathering and acknowledging that gathering such intelligence may require the adoption of extraordinary measures and approaches,[1] international human rights law ascribes limits to how such extraordinary measures can be used. First and foremost, intelligence collection, by its very nature, is likely to infringe aspects of the right to privacy that all individuals enjoy under international human rights law. However, there are six accepted grounds in international law under which it may be acceptable to interfere with an individual's or group's privacy: National security, public safety, the

[1] For example, see 'Report of the UN High Commissioner for Human Rights on the protection of human rights and fundamental freedoms while countering terrorism', UN Doc. A/HRC/16/50.

economic wellbeing of the country, the prevention of disorder or crime, protection of public health or morals, and the protection of the rights and freedoms of others. All but public health and morals fall squarely within an intelligence service's purview. While there is a growing body of jurisprudence on the use of so-called Special Investigation Techniques by law enforcement and domestic security agencies – for instance, telephone intercepts, eavesdropping devices, surveillance tools, undercover operations and human source recruitment – there is far less jurisprudence that touches upon the collection of foreign intelligence although perhaps some basic principles can be inferred from court rulings, as well as other international bodies, particularly regarding mass data collection.

The UN's Human Rights Committee has noted that any law authorizing interference with an individual's right to privacy must itself comply with the provisions, aims and objectives of the International Covenant on Civil and Political Rights (ICCPR).[2] The Human Rights Committee also added that the reference in Article 17 to 'arbitrary interference' had been introduced intentionally 'to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances'.[3] In the case of *Toonen v. Australia*, the Committee has further interpreted the concept of reasonableness in this context to indicate 'any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case'.[4] The UN Office of the High Commissioner for Human Rights has further emphasized that States have an obligation to protect against the arbitrary exercise of Special Investigation Techniques.[5]

In *Klass v. Germany* (1978) the European Court of Human Rights stated that any system of secret surveillance conducted by the State must be accompanied by adequate and effective guarantees against abuse.[6] More recently in *Szabó and Vissy v. Hungary* (2016) the Court ruled that the 2011 National Security Act introduced by the Hungarian government

---

[2] UN Human Rights Committee (1994), 'General Comment 16', UN Doc. HRI/GEN/1/Rev.1 at 21, para. 3.

[3] Ibid., para. 4.

[4] Human Rights Committee (1994), *Toonen v. Australia*, Communication No. 488/1992, UN Doc. CCPR/C/50/D/488/1992, para. 8.3.

[5] Office of the High Commissioner for Human Rights (2008), *Human Rights, Terrorism and Counter-terrorism, Fact Sheet No. 32* (July 2008), at 45.

[6] *Klass v. Germany*, App. no. 5029/71 (ECtHR, 6 September 1978), para. 50.

conferred powers on State agents so overly broad and ill-defined that they could target 'virtually anyone',[7] commenting further: 'A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding of democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation'.[8] The use of 'strict' and 'vital' clearly signals the Court's intention to set a very high threshold.

But, it should be noted, the cases cited above all refer to domestic intelligence gathering and so the extent to which they also impact foreign intelligence operations is still open to considerable debate. Perhaps the most that can be said is that foreign intelligence operations must be necessary, proportional, and precisely targeted in their effect; intelligence activities should be regulated by domestic law; they cannot abuse an individual's fundamental human rights; and a criminal act committed for intelligence purposes is still a criminal act, and any country possessing sufficient jurisdiction is well within its rights to bring the perpetrator to justice. The latter point is the principle reason why so many intelligence officers serve overseas under diplomatic cover – should an operation go wrong, as in the case of the alleged Central Intelligence Agency (CIA) officer Ryan Fogle detained in Moscow in May 2013,[9] the diplomatic immunity afforded by their cover position is the only thing that keeps them out of jail.

It follows therefore that governments assume and accept that both their own foreign intelligence services – and those of other States – will act illegally in the interest of national security in that they will try to gain information to which they have no legal right of access. But this should not set a different standard between domestic and foreign intelligence services when it comes to international obligations under human rights law. It is a legal curiosity that whereas the US Constitution and a large body of US law protects US citizens from intrusive or abusive action by their own government, wherever they are in the world, it does not afford the same protections to the citizens of other countries. For example, a US launched drone strike on a US citizen abroad reportedly requires a higher

---

[7] *Szabó and Vissy v. Hungary*, App. no. 37138/14 (ECtHR, 12 January 2016) para. 89

[8] Ibid., para. 73

[9] Fogle was arrested while allegedly attempting to recruit a Russian counter-terrorism official and subsequently declared persona non grata.

standard of justification and a higher level of clearance than an attack on a non-US citizen. Similarly, although the CIA interpreted its authority to counter the al Qaeda threat following the attacks of 9/11 to include kidnap, illegal detention and 'enhanced interrogation techniques' that were later considered torture, it took care to conduct these operations abroad and against non-US citizens. Not only are these double standards ethically wrong, but the actions themselves remain, prima facie illegal under international human rights law.

Leaving these egregious examples aside, while intelligence officers operating overseas do sometimes break foreign law in pursuit of their country's national interest, it does not automatically follow that all intelligence officers are scofflaws who will stop at nothing to secure their objective. The other side of the coin is that intelligence officers also work in a highly controlled environment. To obtain and maintain a security clearance requires a certain amount of moral rectitude and a lifetime of law abiding behavior. As in the military sphere, legal advisers often play a critical role in the planning of intelligence operations. Effective parliamentary oversight, where it exists, ensures an element of accountability. The modern intelligence officer is painfully aware that he longer works entirely in the shadows.

Nonetheless, in the context of the post-9/11 conflict against Al Qaeda and its affiliates and successors, intelligence personnel have come under more pressure than ever to achieve results and this has led some western intelligence officers to commit well-documented human rights abuses. To be crystal clear, this is both illegal and indefensible, and when such incidents occur States have an obligation to investigate them and bring the perpetrators to justice. But to borrow a well-worn aphorism, it is also worse than a crime, it is a blunder. As we will seek to demonstrate below, it is also clearly possible to collect intelligence on potential terrorism threats both at home and abroad entirely within the boundaries of existing human rights law. While history offers plenty of examples of intelligence agencies around the world that have exceeded these boundaries, it is also replete with evidence that such activity was both unproductive and unnecessary.

1. HUMAN SOURCES AND INTERNATIONAL HUMAN RIGHTS LAW

A human intelligence asset can be the most valuable of all intelligence sources, and it is the threat that terrorist organizations tend to fear the

most.[10] The Brazilian revolutionary Carlos Marighella took care to warn readers of his *Minimanual of the Urban Guerrilla* that 'the worst enemy of the urban guerrilla and the major danger we run is infiltration into our organization by a spy or informer'.[11] The reason for this concern is pretty self-evident – unlike more passive intelligence collection methods, a human source is dynamic, responsive to direction, and, above all, sentient. Such a source can offer insights other intelligence assets cannot, and, as Marighella noted, they come in two basic varieties – informants, private individuals already associated with the target, and spies, agents of the State who successfully manage to infiltrate a target group or operation. While infiltrating a trained agent or an undercover officer into an organization can be both more dangerous and more difficult than recruiting an informant who is already inside or close to it, the advantage of manoeuvring a directed source or a professional officer into such a position is that they tend to be substantially more reliable assets in the field and to have a great deal more credibility in court.

There is nothing in international human rights law to prevent State agencies from using either informants or spies, indeed it is actively encouraged by international institutions. The United Nations Convention against Transnational Organized Crime (UNTOC) encourages State parties to make use of participating informants in the investigation of organized crime groups, and the same logic can be applied to terrorist groups.[12] However, human intelligence operations are governed by the same human rights obligations as any other special investigation technique – recruiters cannot commit human rights violations, criminal acts, blackmail or threaten suspects to gain their cooperation. In addition, acting as an informant on or inside a terrorist group is inherently dangerous and the State has an obligation under human rights law to protect the life and security of its asset.

---

[10] It is worth noting that structured terrorist organizations almost invariably create a counter-intelligence department early on as part of their central directorate.

[11] Carlos Marighella (1970), *Minimanual of the Urban Guerrilla* (Havana: Tricontinental).

[12] Article 26 of the UN Convention against Transnational Organized Crime (UNTOC). See UN Office on Drugs and Crime (UNODC), Terrorism Prevention Branch (2014), 'Counter-Terrorism Legal Training Curriculum: Module 4 Human Rights and Criminal Justice Responses to Terrorism', https://www.unodc.org/documents/terrorism/Publications/Module_on_Human_Rights/Module_HR_and_CJ_responses_to_terrorism_ebook.pdf, accessed 11 October 2017, p. 91.

It is not uncommon for an informant operating in a criminal milieu to be put in a position where he or she may be expected by criminal confederates to commit a criminal act or risk exposure. States may therefore promise an informant immunity from prosecution should they be asked to participate in certain acts. The UNODC Model Legislative Provisions against Organized Crime, which are intended to assist States in implementing UNTOC, offer some guidance on the type of activities that an informant (or for that matter an undercover officer) infiltrated into a criminal group might reasonably undertake without being held criminally responsible, such as making available 'legal and financial means, transport, storage, housing and communications needed for the perpetration of those offences'.[13]

However, there is a limit to which a human intelligence asset can lawfully transgress laws in the public interest. International human rights law also places important restrictions on the activities of an informant acting under the direction of the State or its representatives – even when an informant is working for the authorities it is completely impermissible for him or her to participate in the abuse of fundamental human rights, such as acts involving killing, enforced disappearance or torture and ill-treatment, since the 'prohibition on torture and the arbitrary deprivation of life are absolute and cannot be justified, even by reference to important law enforcement goals such as the investigation of terrorism'.[14] Immunity must not lead to impunity where serious human rights violations are at stake.[15] It should also be stressed that the practice of the various international criminal tribunals has established the general principle under international criminal law that no one can be granted immunity from prosecution for involvement in war crimes, crimes against humanity, genocide or acts of torture.

There is no shortage of modern examples of law enforcement and intelligence agencies recruiting or turning members of terrorist groups and putting them back to work in the service of the State. British intelligence enjoyed considerable success in penetrating the Provisional

---

[13] 'Counter-Terrorism Legal Training Curriculum', ibid., at 93. See also UNODC (2012), Model Legislative Provisions against Organized Crime, https://www.unodc.org/documents/organized-crime/Publications/Model_Legislative_Provisions_UNTOC_Ebook.pdf, accessed 11 October 2017, at Article 15, paragraph 3.

[14] 'Counter-Terrorism Legal Training Curriculum' (n 12), at 93.

[15] Organization for Security and Cooperation in Europe (2007), *Countering Terrorism, Protecting Human Rights: A Manual* (Warsaw: OSCE/ODIHR), p. 144.

IRA despite the close-knit world of Irish republicanism. In the mid 1980s British military intelligence officers recruited a former Provisional IRA Quartermaster called Frank Hegarty who was aggrieved about his dismissal from his clandestine post by the local IRA commander in Londonderry, Martin McGuinness. The surprisingly moralistic McGuinness disapproved of Hegarty leaving his wife for his mistress. After Hegarty was able to worm his way back into the IRA's good graces he provided crucial intelligence on a major arms shipment sent to the Provisional IRA by Libya's Colonel Gaddafi.[16] Perhaps one of Britain's most significant successes was the recruitment of Denis Donaldson, a former Provisional IRA gunman who had taken part in the 1970 Short Strand gun battle between republicans and loyalists, and had been incarcerated in Long Kesh prison for terrorism-related offences. He also acted as one of the Provisional IRA's go-betweens with terrorist groups in Lebanon, including Hezbollah. In the 1990s he became a prominent figure in Sinn Fein and in 2000 was appointed the administrator for the party's bloc in the Northern Irish Assembly. He was well placed to pass crucial insights on republican positions to the British government as it negotiated the Good Friday Agreement that helped bring the conflict in Northern Ireland to an end. Donaldson publicly confessed to his role as an informer in December 2005, and was murdered by the Real IRA four months later.

British intelligence has also reportedly enjoyed some success infiltrating Al Qaeda. One apparent case that has received considerable publicity is that of Aimen Dean, a young Saudi who fought in Bosnia as a mujahedin volunteer alongside Bosnian government forces before being drawn into the orbit of Al Qaeda where he became a religious counselor working with the organization's new recruits. By his account, Dean began to question the legitimacy of Al Qaeda's use of terrorist violence in the aftermath of the 1998 attacks on the US embassies in Nairobi and Dar-es-Salaam, which killed many innocent local citizens in addition to US embassy staff. Seeking guidance from Al Qaeda's senior religious adviser, Abu Abdullah al-Muhajir, he found the arguments used to justify the collateral injury to innocent civilians, grounded as they were in a thirteenth-century fatwa written in response to Mongol incursions into Muslim lands, completely unconvincing and began to turn away from the organization. He left to the Gulf for medical treatment at the end of 1998 privately determined to leave Al Qaeda and while he was there, he says

[16] Stephen Grey (2015), *The New Spymasters: Inside Espionage from the Cold War to Global Terror* (New York: St Martin's Press), pp. 76 and 77.

he was approached by the Secret Intelligence Service (SIS) and ultimately recruited. After a number of months being debriefed by British intelligence officers he was asked if he would be prepared to go back to Al Qaeda and act as an informer. Dean says he agreed to the plan and remained an active intelligence source for many years. In an interview with the BBC conducted in 2015 Dean was asked if he had had any moral qualms about betraying his former comrades:

> Whatever moral misgivings I had, I have my ex-comrades to thank for driving those moral misgivings away because the more I saw what they were planning – for example, I was there basically when al-Qaeda was constructing their first workable chemical device and talking about this with such glee and such deep psychopathic satisfaction … that is when you say to yourself, 'Why do I have any moral misgivings about spying on you guys?' Whatever they are doing is justifying whatever you are doing.[17]

Morten Storm, also known as Murad Storm Al-Denmarki, is another interesting case. After a troubled childhood, Storm joined the Bandidos motorcycle gang. He also became interested in Islam after coming across a biography of the Prophet Mohammed in his local library. He was arrested in 1997, befriended a Danish convert to Islam in prison and began to become more serious about his faith, which led him into extremist circles in both Denmark and the UK. Over time he also became friendly with Anwar al-Awlaki, the US-born religious scholar who would become the spiritual adviser to Al Qaeda in the Arabian Peninsula. In this period he says he was approached by several western intelligence agencies but rebuffed them all. But after he found his path to joining the Islamic Courts Union in Somalia blocked by Ethiopian troops gaining control of Mogadishu airport he began to question God's purpose for him. Storm eventually began to reject the extremist narrative promoted by his friends: 'Now I thought of the twin towers, Bali, Madrid in 2004, London in 2005 … If they were part of Allah's preordained plan, I now wanted no part of it … My loss of faith was as frightening as it was sudden … I was the convert unconverted'.[18] Storm sought out the Danish Security and Intelligence Service (PET) and offered to spy on his former comrades for them – in doing so, Storm became a distinct type of human intelligence asset known in the jargon of espionage as 'a volunteer'.

---

[17] Peter Marshall (2015), 'The spy who came in from al-Qaeda', BBC News Magazine, 3 March, http://www.bbc.com/news/magazine-31700894, accessed 21 October 2015.

[18] Morten Storm (2014), *Agent Storm: My Life Inside Al Qaeda and the CIA* (New York: Atlantic Monthly Press) pp. 118 and 122.

According to Storm, the Danes were delighted to take him up on his offer, and introduced him to British and American intelligence officers. Storm claims that it was his information that enabled the US to establish the whereabouts of al-Awlaki in Yemen.

Having an asset in place who holds the trust of terrorist group members opens up further possibilities beyond the simple acquisition of intelligence, it can allow law enforcement and security agencies to disrupt terrorist plots before they escalate to the point at which the public is put at risk. A tactic often favored by the authorities is the sting operation, in which aspiring terrorists are unwittingly given the space by a person they trust to incriminate themselves in tightly controlled circumstances, such as an arms deal or a planned attack. When the British Security Service (MI5) learned in 2001 that the Real IRA was looking for a 'rogue State' to sponsor its operations,[19] MI5 officers posing as representatives of the Iraqi Intelligence Service met with members of the Real IRA in Dublin, Slovakia, Austria and Budapest before triggering an arms sting in Piest'any, Slovakia, that resulted in the arrest and subsequent conviction of three of the organization's members: Fintan O'Farrell, Declan Rafferty and Michael McDonald. Operation Samnite was the first MI5 operation in which evidence was gathered entirely overseas and it still stands out today as an exemplar of the power of international cooperation.[20]

In undercover operations and sting operations any individual acting under the direction of the authorities – law enforcement officers, intelligence officials, police informants or intelligence assets – must be careful to avoid any situation in which they become the instigator or agent provocateur behind a crime – such action on the part of the authorities is entrapment. Entrapment occurs when a person who would not otherwise be predisposed to commit an offence is encouraged to do so by a government official who then instigates prosecution against the same individual. On 26 November 2010, accompanied by an undercover FBI Special Agent, Mohamed Osman Mohamud, a Somali-American student at Oregon State University, tried to detonate a car bomb near a public Christmas tree lighting ceremony in Portland's Pioneer Courthouse Square attended by thousands of families. The bomb had been constructed with the FBI's help from inert material and did not explode. However, Mohamud did not know this and made a triggering call from

---

[19] Jason Bennetto (2002), 'Irish terrorists captured in MI5 sting plead guilty', *The Independent*, 3 May.

[20] Richard Norton-Taylor (2002), '30 years in jail for Real IRA trio', *The Guardian*, 8 May.

his cellphone to the bomb's detonator. He was then arrested. Mohamud had first come to notice because he had made contact with a suspected Al Qaeda recruiter in the Middle East, and because he had written an article on physical fitness for an English-language publication called *Jihad Recollections*. An undercover FBI Special Agent made contact with Mohamud in June 2010 posing as a terrorist. In early November 2010, undercover FBI agents traveled to a remote location with Mohamud for a trial run of the bombing in which Mohamud actually detonated a functional backpack bomb.

In a pre-emptive strategy in the Pioneer Courthouse Square case, to rebut allegations of entrapment the FBI agents deliberately offered Mohamud multiple less violent alternatives to take action in support of Al Qaeda's cause, including prayer, but Mohamud insisted he wanted to play an 'operational' role. In an affidavit, the FBI stated that Mohamud chose the venue for the attack and also shrugged off attempts to derail the plot when it was under way. US Attorney General Eric Holder told reporters: 'There were a number of opportunities the defendant was given to retreat and to take a different path and he chose at every step to continue'.[21] Mohamud was reportedly told several times that his planned bomb could kill women and children but he told agents: 'Since I was 15 I thought about all this … It's gonna be a fireworks show … a spectacular show'.[22]

The European Court of Human Rights has explored the question of entrapment in some detail. Two cases in particular, both relating to drug purchases, illustrate the basic principle at work quite clearly: *Francisco Teixeira de Castro v. Portugal* and *Grigoriy Arkadyevich Vanyan v. Russia.* In the Portuguese case a textile worker was offered money by two plainclothes police officers to supply them with heroin. Although he had no previous criminal record, Mr Teixeira de Castro did have the necessary contacts to obtain the drug.[23] Tempted by the money, the applicant accepted the officers' request and was subsequently charged and convicted of a drug offence. In reviewing the case the Court concluded that the officers 'did not confine themselves to investigating Mr. Teixeira de Castro's criminal activity in an essentially passive manner, but exercised an influence such as to incite the commission of

---

[21] Dina Temple-Raston (2010), 'Alleged Portland bomber to claim entrapment', National Public Radio, 30 November, http://www.npr.org/2010/11/30/131704930/alleged-portland-bomber-to-claim-entrapment, accessed 7 June 2017.

[22] Liz Robbins and Edward Wyatt (2010), 'Somali-born teenager held in Oregon bomb sting', *New York Times*, 27 November.

[23] *Teixeira de Castro v. Portugal*, App. no. 44/1997/828/1034 (ECtHR, 9 June 1998).

the offence'.[24] The Russian case is very similar except that in this instance it was a police informant, rather than a police officer, who encouraged the suspect to make a drug purchase.[25] The 'passivity' standard set by the European Court essentially prohibits the authorities from playing any kind of active role in the commission of a criminal act as a pretext to making an arrest. Any evidence obtained as a result of police incitement must be excluded from trial.[26]

One final tactic often used in human intelligence operations is disruption – a concept as simple as it is efficient. Disruptions are non-judicial interventions designed simply to upset a terrorist group's plans. A disruption might be as simple as increasing the security presence around a target or releasing advance warning of an attack to the media, so that a terrorist cell is panicked into aborting its operation. On occasion, the authorities might even approach the suspect directly and warn him or her that the State is aware of their plans knowing that this leaves them with little choice but to abandon them. After the bombing of the Khobar Towers housing facility in Dhahran, Saudi Arabia, by a Saudi offshoot of Hezbollah, which killed 19 Americans in June 1996, the Clinton White House debated many military and non-military responses against Iran. One response that was implemented consisted of a large-scale covert operation that 'outed' Iranian agents around the world, putting them on notice that their affiliation was known to US intelligence, in order to deter Tehran from threatening US facilities. Among the participants was then-CIA station chief to Saudi Arabia John Brennan, who reportedly knocked on the car window of an Iranian intelligence officer, and announced: 'Hello, I'm from the U.S. embassy, and I've got something to tell you'.[27] The Iranian was left knowing his cover was blown, and wondering just how much the US knew about his activities and how badly his operational security had been compromised. For an operative in the field such uncertainty can be paralyzing.

---

[24] Ibid., paras. 37 and 38.

[25] *Vanyan v. Russia*, App. no. 53203/99 (ECtHR, 15 March 2006), paras. 45–50.

[26] *Ramanauskas v. Lithuania*, App. no. 74420/01 (ECtHR, 5 February 2008), para. 60.

[27] George Tenet (2009), *At the Center of the Storm* (New York: HarperCollins).

2. INTELLIGENCE AGENCIES AND TORTURE

The use of torture, or cruel, inhuman or degrading treatment, to compel suspects in custody to divulge information is not an approach most intelligence officers in the western world would consider to have any place in their profession. However, it is also an incontrovertible fact that some western intelligence and security agencies, just like some western military and police organizations, have made the mistake of experimenting with such tactics in their struggle with terrorist groups of one sort or another. They have gained little intelligence and lost much credibility by doing so, as the sordid story of the CIA's 'enhanced interrogation' program following the attacks of 9/11 demonstrates only too clearly.[28]

Proponents of torture often contend that it gets results that cannot be obtained using lawful techniques. The counterfactual is of course impossible to prove one way or another in any individual case, but while undoubtedly some people may cooperate under duress, the historical record also clearly shows that others do not. Professor Darius Rejali noted in an extensive study of the Gestapo's use of torture that this most brutal of organizations failed to break senior leaders of French, Danish, Polish and German resistance,[29] and that, compared to the information generated from public cooperation and informers, the leads gained from torture were, to quote an internal Gestapo report, 'pathetic'.[30] There are many other well-documented examples of members of armed groups resisting coercive interrogation.

The use of torture during the Battle of Algiers in 1957, fought between the French military and the indigenous Algerian independence movement led by the *Front de Libération Nationale* (FLN), is often held up as an example of torture being used to good effect to counter terrorism, but the historical record is rather more complicated than its advocates would

---

[28] The CIA use of 'enhanced interrogation techniques' was examined in detail by the US Senate Select Committee on Intelligence (SSCI), 'Committee Study of the Central Intelligence Agency's Detention and Interrogation Program', released on 9 December 2014, available at http://www.intelligence.senate.gov/study2014/sscistudy1.pdf, accessed 8 May 2017. See also UN Human Rights Council (2010),'Joint study on global practices in relation to secret detention in the context of countering terrorism of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism', UN Doc. A/HRC/13/42.

[29] Darius Rejali (2007), *Torture and Democracy* (Princeton: Princeton University Press), p. 496.

[30] Darius Rejali (2007), '5 myths about torture and truth', *The Washington Post*, 16 December. See also Rejali (n 29).

have one believe. To be sure, some individuals tortured in French custody undoubtedly provided some useful information. However, as one French interrogator acknowledged, it was still difficult to separate the wheat from the chaff: 'Just as the interrogation starts they speak abundantly, cite the names of the dead or militants on the lam, indicate the placement of an old arms cache in which we will find only a couple of documents without interest'.[31] Furthermore, the FLN hierarchy knew that the men under its command faced torture if captured and moved to exploit the situation by instructing its fighters to give up the names and locations of their more moderate rivals in the *Mouvement National Algérien* (MNA).[32] The French were thus goaded into torturing MNA members, which only served to push their colleagues into the embrace of the FLN.[33]

In 2001 the former French intelligence officer Paul Aussaresses provoked an outcry in France by publishing a memoir, entitled *Services Spéciaux*, in which he described the harsh treatment he had meted out to the FLN operatives unlucky enough to fall into his hands: 'Beatings, electric shocks, and, in particular, water torture, which was the most dangerous technique for the prisoner'.[34] Aussaresses recalled one instance in which a prisoner died while being waterboarded without revealing anything of value with a chilling lack of remorse: 'I had no regrets over his death – if I had any regrets, it was because he did not talk'.[35] It wasn't the only time he failed to make someone talk – he admitted somewhat grudgingly in his memoir that his victims 'would talk either quickly or never'.[36] There wasn't much that Aussaresses was not prepared to do to someone unlucky enough to be placed in his custody, so we can take it from a very accomplished torturer that a willingness to torture does not guarantee results. Indeed, one of those apprehended by Aussaresses and his men was the editor of the pro-independence communist newspaper *Alger Républicain*, Henri Alleg. Despite being subjected to electric shocks and water torture, burned, beaten, and drugged with sodium pentothal, Alleg famously did not give up the name of the

---

[31] Rejali (n 29), at 481.

[32] National Algerian Movement.

[33] Rejali (n 29), at 481 and 482.

[34] Paul Aussaresses (2002), *The Battle of the Casbah: Terrorism and Counterterrorism in Algeria 1955–1957* (New York: Enigma Books), p. 128. *The original French title was Services Spéciaux: Algérie 1955–57.*

[35] Adam Shatz (2001), 'The Battle of Algiers', *The Nation*, 18 June, http://www.thenation.com/article/battle-algiers-0/, accessed 30 December 2015.

[36] Aussaresses (n 34), at 128.

individual who had hidden him from the authorities.[37] Henri Alleg's account of his treatment in French custody, *La Question*, published in 1958, became an international sensation.[38]

Despite the FLN's sly tactics and the bravery of individual captives, torture may have helped briefly to tip the balance in France's favor during the Battle of Algiers, but it is important to note that it did so at a profound strategic cost. The use of torture further radicalized Algerian Arabs, it alienated the French public, it contributed to the political collapse of the Fourth Republic, and it eroded good order and discipline within the French army to the point that disgruntled military personnel led two abortive coup attempts in 1958 and 1961. French military veterans also established the nativist terrorist group, the *Organisation de l'Armée Secrète* (OAS), and later the *Conseil National de la Résistance* (CNR)[39] which attempted to assassinate French President Charles de Gaulle on several occasions.[40] Algeria gained its independence in 1962, following a referendum in which 99.72 percent of those taking part (most European settlers had already left for France) voted in favor.

The *ne plus ultra* of the utilitarian argument in favor of torture is the ticking bomb thought-experiment.[41] Paul Aussaresses summarized the argument in *Services Spéciaux*: 'Just think for a moment that you are personally opposed to torture as a matter of principle and that you have arrested a suspect who is clearly involved in preparing a violent attack. The suspect refuses to talk. You choose not to insist. Then the attack takes place and it's extremely bloody. What explanation will you give to the victim's parents, the parents of a child, for instance, whose body was torn to pieces by the bomb, to justify the fact that you didn't use every method available to force the suspect into talking'.[42] As a thought-experiment the ticking bomb scenario dispenses with all the complications that make the real world so difficult to navigate, and as such it may provoke an interesting philosophical discussion but it has little value

---

[37] See Henri Alleg (1958), *The Question* (New York: George Braziller Inc.).

[38] Available at http://www.tandfonline.com/doi/abs/10.1080/09546550701476141?journalCode=ftpv20, accessed 11 October 2017.

[39] National Council of Resistance.

[40] Paul Henissart (1970), *Wolves in the City: The Death of French Algeria* (New York: Simon and Schuster), pp. 475 and 476.

[41] Rod Morgan and Tom Williamson (2009), 'A critical analysis of the utilitarian case for torture and the situational factors that lead some people to become torturers', in Tom Williamson et al., *International Developments in Investigative Interviewing* (Abingdon: Routledge), p. 131.

[42] Aussaresses (n 34), at p. 41 of ebook.

as a tool for analyzing public policy. In the fantasy constructed by Aussaresses and his fellow enthusiasts you always have the right suspect in custody, the bomb is always real, the suspect always has the information you need, the suspect always talks when tortured, and the information the suspect then provides is always sufficiently accurate and detailed to avert the looming catastrophe. However, as Bob Brecher points out in *Torture and the Ticking Bomb*, in the real world none of these variables is quite so assured.[43]

Torture is a very blunt tool. Interviewers rarely have all the facts at their disposal when conducting interviews and a discursive, rapport-based interview technique is much more likely to assist the interviewer successfully navigate complex narratives of which he often has limited prior knowledge because it allows the subject to introduce new information into the conversation, and correct misapprehensions and flawed intelligence. Physical abuse creates a very different dynamic. The torturer sets the boundaries of the interview and it is driven forward by the knowledge he or she already possesses, and the assumptions he or she has made. The torturer is mostly reduced to asking closed questions, which further confines and restricts his or her exchange with the prisoner. French paratroopers were able to use torture with some initial intelligence-gathering success in the Battle of Algiers because they were seeking very specific information – a name or a location – and closed questions can at least adequately support this objective if the information the interrogator has at the outset of the interrogation is accurate. As one French veteran of Algeria admitted: 'A profound knowledge of the [terrorist] organization is required. It is useless to ask a funds collector about caches of weapons or bombs'.[44]

In addition, the attraction to acts of wanton cruelty that lurks inside some human beings is another important consideration. The patina of legitimacy imparted by superior orders often liberates dark impulses – the social psychologist Philip Zimbardo famously dubbed this phenomenon the 'Lucifer Effect'.[45] The reality is that much of the abuse that takes place in the interview room is driven by the frustration of the interrogators themselves – or in the immediate aftermath of an incident by anger at the perpetrators – rather than by any genuine calculation that

---

[43] See Bob Brecher (2007), *Torture and the Ticking Bomb* (Oxford: Blackwell Publishing).

[44] Roger Trinquier (1964), *Modern Warfare: A French View of Counter-insurgency* (London: Pall Mall Press), p. 23.

[45] See Philip Zimbardo (2007), *The Lucifer Effect: Understanding How Good People Turn Evil* (New York: Random House).

abuse will result in getting the suspect in front of them to share the information they need.

For all these reasons and more, the utilitarian debate about torture is not a simple equation in which one guilty man's pain is the price paid to protect the wider population, as the Georgetown Professor of Law and Philosophy David Luban has cogently observed, 'it is the debate between the certainty of anguish and the mere possibility of learning something vital and saving lives'.[46] The celebrated French author Albert Camus, who was born and raised in Algeria and was deeply affected by the brutal conflict between the FLN and French settlers, further noted that an act of torture does not occur in a vacuum: 'Torture has perhaps saved some, at the expense of honor, by uncovering thirty bombs, but at the same time it arouses fifty new terrorists who, operating in some other way and in some other place, will cause the death of even more innocent people'.[47] This is no mere literary flight of fancy.

It is now a relatively uncontroversial observation that the US adoption of so-called 'enhanced interrogation techniques' proved to be a profound misstep that generated little intelligence and provided Al Qaeda with a propaganda windfall – the US treatment of prisoners was mentioned 32 times in Al Qaeda propaganda messages between 2003 and 2010, and by affiliate groups 26 times.[48] The first issue of the online magazine *Inspire*, published by Al Qaeda in the Arabian Peninsula in the summer of 2010, featured an essay by Osama bin Laden in which he specifically referenced 'the crimes at Abu Ghraib and Guantanamo, those ugly crimes which shook the conscience of humanity'.[49] US General David Petraeus, former Director of the CIA and commander of US forces in both Iraq and Afghanistan, had presciently observed in an interview earlier the same year: 'Abu Ghraib and other situations like that are non-biodegradable. They don't go away. The enemy continues to beat you with them like a stick'.[50] Mark Fallon, a US Naval Criminal Investigative Service (NCIS)

---

[46] David Luban (2006), 'Liberalism, torture and the ticking bomb', in Karen Greenberg (ed.), *The Torture Debate in America* (New York: Cambridge University Press), pp. 46 and 47.

[47] Albert Camus (1963), 'Preface to Algerian Reports', in Albert Camus, *Resistance, Rebellion and Death* (New York: Modern Library), p. 84.

[48] James Gordon Meek (2010), 'Gitmo fades as "recruiting tool for Al Qaeda"', *New York Daily News*, 25 January.

[49] Thérèse Postel (2013), 'How Guantanamo Bay's existence helps Al-Qaeda recruit more terrorists', *The Atlantic*, 12 April.

[50] Joseph Berger (2010), 'U.S. Commander describes Marja Battle as first salvo in campaign', *New York Times*, 21 February.

special agent who led the task force investigating the 2000 bombing of USS Cole and was a close colleague of the FBI agent Ali Soufan, who demonstrated that harsh treatment in that case added nothing to prior knowledge,[51] put it even more starkly, writing in 2014: 'It enabled – and, in fact, is still enabling – al Qaeda and its allies to attract more fighters, more sympathizers, and more money'.[52]

The use of torture and other forms of cruel, inhuman and degrading treatment by the US in this period also created significant ethical and legal dilemmas for some of its closest allies and European support for US counter-terrorism measures was drastically impacted by policies that clearly violated the European Convention on Human Rights.[53] Perhaps the most dramatic example of this was the *in absentia* conviction of 23 US agents in an Italian court for the role they played in the extraordinary rendition of radical Imam Hassan Mustafa Osama Nasr from Milan to Cairo in 2003.[54] Nine Italian officials, including two senior officers of the *Servizio per le Informazioni e la Sicurezza Militare* (SISMI),[55] also faced prosecution in the case. In 2012, Polish prosecutors charged the former head of Polish intelligence, Zbigniew Siemiatkowski, with 'unlawfully depriving prisoners of the their liberty' because of the alleged role he played in helping to establish a CIA black site in Stare Klejkuty, north-eastern Poland, in 2002–2003.[56] The Polish President at the time, Aleksander Kwasniewski, later ruefully admitted: 'We had concerns, but they did not include that the Americans would break the law in a knowing and uncontrolled way'.[57] The possibility of being held legally

---

[51] See Ali H. Soufan (2011), *The Black Banners* (New York: W.W. Norton & Company).

[52] Mark Fallon (2014), 'Dick Cheney was lying about torture', *Politico Magazine*, 8 December, http://www.politico.com/magazine/story/2014/12/torture-report-dick-cheney-110306.html#.VbvcDpNVikp, accessed 8 January 2016.

[53] Intelligence and Security Committee (2007), 'Rendition', July, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/224654/rendition.pdf, accessed 11 October 2017, at pp. 12 and 13.

[54] See Steve Hendricks (2010), *A Kidnapping in Milan: The CIA on Trial* (New York: W.W. Norton & Company).

[55] Military Intelligence and Security Service.

[56] Joanna Berendt and Nicholas Kulish (2012), 'Polish ex-official charged with aiding CIA', *The New York Times*, 27 March.

[57] The Economist (2014), 'Detention site blues: Poles are not happy about CIA torture, but they need America too much to start a row', 11 December, https://www.economist.com/news/europe/21635984-poles-are-not-happy-about-cia-torture-their-soil-they-still-need-america-detention-site-blue, accessed 11 October 2017.

liable for the criminal acts of an allied power has inevitably had a chilling effect on the predisposition of some US allies to work so closely with their American counterparts. The British authorities have been surprisingly open about the difficulties that policies such as rendition to torture and the operation of secret prisons have caused the transatlantic 'special relationship'. The then Director General of MI5 Dame Eliza Manningham-Buller acknowledged in testimony before the Parliamentary Intelligence and Security Committee (ISC) in 2007: 'We certainly now have inhibitions … greater inhibitions than we once did'.[58] Sir John Scarlett, then Chief of SIS, similarly reported that his agency sought 'credible assurances' that any action taken by the US on the basis of intelligence provided by UK agencies would be 'humane and lawful' and that when such assurances were lacking 'we cannot provide the information'.[59]

Darius Rejali has noted that there are essentially only three reasons for a State to employ torture: 'to intimidate, to coerce false confessions, and to gather accurate security information'.[60] Torturers may, through the exercise of brutality, successfully achieve the first two of these goals, but the record shows that as a means for collecting accurate information torture is unreliable, and its use comes at great personal, reputational and moral costs that can have a profoundly detrimental impact on counter-terrorism efforts by undermining popular support for the State, antagonizing key constituencies, and alienating much needed allies. This was certainly the experience of the US, which paid a high price for what comprehensive investigation has since established was an almost entirely unproductive policy.[61] When President Obama came into office in January 2009 one of his first actions was to issue Executive Order 13491 to improve the effectiveness of human intelligence gathering and to promote the safe, lawful, and humane treatment of individuals in US custody.[62] This executive order put a formal end to the use of so-called enhanced interrogation techniques and restricted the intelligence community to methods authorized and listed by the US Army Field Manual on Human Intelligence Collector Operations. Speaking at Fordham University in March 2010, Michael Sulick, then head of the CIA's

---

58 Intelligence and Security Committee (n 53), at 47.
59 Ibid.
60 Rejali (n 29), at 23.
61 See, inter alia, SSCI (n 28).
62 Barack Obama (2009), Executive Order 13491 – Ensuring Lawful Interrogations, The White House, 22 January, https://www.whitehouse.gov/the_press_office/EnsuringLawfulInterrogations, accessed 9 January 2016.

National Clandestine Service, told his audience 'I don't think we've suffered at all from an intelligence standpoint' because of this decision.[63]

3. HUMAN RIGHTS ISSUES SURROUNDING THE DISSEMINATION AND USE OF INTELLIGENCE

Regardless of the method of its acquisition, the use of intelligence can also give rise to human rights considerations. If intelligence is not used, it has no value. This may seem obvious, but the collector of intelligence is often far more concerned about the method of collection and the importance of protecting the source, than about the potential impact of the intelligence if disseminated. The most secure option will be to prevent all dissemination, and if the value of the information appears marginal and without immediate relevance, a decision to store the information without dissemination may be the most sensible course of action. Even when the information may have immediate value and relevance, if any action taken as a result could lead to the exposure of the source, then again the right decision may be to hold onto it until some collateral can be developed or to disseminate it but with restrictions on its use.

A famous example of this in the popular imagination occurred in World War II when the British government, through its successful penetration of the Enigma coding machine used by the German High Command, was thought to have known that the Luftwaffe intended to bomb the city of Coventry in November 1940. It was widely believed that the then Prime Minister, Winston Churchill, decided to suppress the information so as not to risk exposing the most significant intelligence breakthrough since the start of the war, and one that was likely to have a major impact on its outcome, so saving many more lives. In fact, although the code breakers had become aware that a massive bombing raid was in preparation, the target was not clear, with most believing it would be London or the South East of the country. But the myth persists, and usefully illustrates the tensions that can arise between the desire to collect more intelligence and the argument for using what has been collected already, even if it exposes the source.

A similar but real incident that had a major affect on the use of terrorist-related intelligence occurred in December 1988 around the

[63] Jeff Stein (2010), 'CIA's top spy: No losses from waterboarding ban', *Washington Post* Partner blog, 1 April, http://voices.washingtonpost.com/spy-talk/2010/04/cias_top_spy_no_losses_from_wa.html, accessed 8 January 2016.

bombing of Pan American flight 103 over Lockerbie in Scotland, which caused the death of 270 people. It was found that the US Embassy in Helsinki had received an anonymous tip that such an attack might occur on a Pan Am flight from Frankfurt to New York just two weeks beforehand. The Federal Aviation Administration issued a bulletin that the State Department distributed to numerous embassies abroad, but although the Moscow Embassy did make the bulletin available to the entire American community in Moscow (in error), there was a widespread impression in the public mind that the government had only warned its own personnel.

The subsequent enquiry into the attack looked at the issue of public notification at length, and concluded that 'either the information remains closely held by those with a legitimate need to know, or it must be made public'.[64] In other words, there should be no double standard. The Commission acknowledged the importance of credibility and specificity in deciding when to pass on threat intelligence to the public, but was clear in its recommendation that 'The U.S. Government should, as a matter of course and policy, consciously consider the question of notification and carefully review the factors outlined'.[65] As a result, the US government now makes public all terrorist threats to civilian targets that it regards as potentially credible, though it may still withhold specific detail if to release it might jeopardize the source. This reflects the general and common sense principle that all intelligence collection on terrorism has the ultimate objective of saving lives, and that the right to life is a right shared equally by all.

4. HUMAN RIGHTS ISSUES SURROUNDING THE SETTING OF INTELLIGENCE REQUIREMENTS

The decision to disseminate or to withhold intelligence, or to allow its onward use or to forbid it, is always influenced by the reason for collecting it in the first place. In terms of best practice, intelligence requirements are not set by intelligence collectors, but by those policy makers or government agencies that are the potential customers. They must bid for the intelligence resources by arguing the importance of getting the information that they seek. In all western countries, there will

[64] President's Commission on Aviation Security and Terrorism (1990), 'Report of the President's Commission on Aviation Security and Terrorism', 15 May, https://archive.org/details/PCASTreport, accessed 11 October 2017, Ch. 6.

[65] Ibid.

be many more requirements than there are resources available to fill them. 'Nice to know' does not make the cut in counter-terrorism, and nor should it. Human assets are not deployed lightly; it is unreasonable to have them risk their liberty or even their lives to collect information of low value. The intelligence requirement must also demonstrate within reason that the information cannot be obtained by overt means.

The intelligence requirement may be for action as well as information, such as the disruption operations mentioned above. But it must also be endorsed by all concerned as within the law, or, if outside the law, of sufficient value to merit an exemption to be provided by a designated official when the opportunity to achieve the objective arises or the planning gets to a point that offers a reasonable chance of success. In the UK this is a government minister or for more routine matters a senior official. In the US requirements are set by the Director of National Intelligence through an inter-agency process known as the National Intelligence Priorities Framework. Other ad hoc requirements emerge from the National Security Staff through a principals committee. At times the president himself will authorize an operation if its consequences may be particularly sensitive or controversial. Congress retains oversight by having control of the necessary budget. But however elaborate the process may be for setting the requirements, the agencies are generally left to decide on their own how best to meet them.

The collectors of intelligence, or those who take the approved counter-terrorist action, are not the only ones required to make a decision about the morality of the means, or the ethical and legal implications of the result. This should be a collective decision by government, as represented by the person signing off the submission or, in the case of the US, the finding. As such the decision becomes the collective decision of the society in whose name the government acts. The proper observance of the fundamental principles of human rights in intelligence requirement setting, intelligence collection and the dissemination of the product, is therefore of wider importance than merely as a way to control abuses by the individual intelligence officer or his customer. Terrorists are by definition people who object to how things are done by the governments they target; and although they aim to challenge public support for government policy by undemocratic means, largely through intimidation, it is important that in responding to the threat of terrorism the government does not reinforce the terrorist narrative that it acts against the public interest. Policies can change, but principles do not.

Terrorism, however, is an area where governments can all too easily abuse and debase the value of their intelligence services and operatives by seeing them as instruments of national politics rather than national

security. Terrorism is too loosely defined in some jurisdictions to ensure that the capacity of the State to act in secret does not lead to abuses of human rights, even to the extent of the extra-judicial killing or incarceration of people in opposition who would not fit the more commonly accepted definitions of terrorism. Here the individual duty of all parties; the politicians, the intelligence services and the consumers of intelligence, must be to uphold international norms and conventions, even though this may require significant acts of individual courage, both moral and physical, in societies, of which there are many, where the organs of State are merely tools that the ruler uses to perpetuate his control.

5. THE SPECIAL ALLURE OF CLASSIFIED INFORMATION

It is reasonable for the customers of intelligence to expect it to tell them something new, important and interesting. This can lead to undue trust being placed in information that is classified because of the method of its acquisition, but not necessarily graded according to its reliability. Rightly or wrongly, something that is acquired at great effort and risk, and stamped secret in large red letters, is likely to have more weight than an analyst's report based on open source information. Unlike the analyst's report, however, an agent who is highly placed within a terrorist organization is likely to produce single source reports that cannot be corroborated by sources elsewhere because his access is unique. His reports may have serious impact on the rights of others; they may result in arrests and detentions, or in serious invasions of privacy, but they may nonetheless be wrong, whether deliberately misconstrued or innocently misreported. The nature of such source reporting makes it very unlikely that there is any meaningful opportunity to cross-examine its originator or even for a willing source to go back and check that what he reported was correct. The briefing, debriefing and examination of the motivation of sources is therefore not just a matter of good agent handling in the context of terrorism, but also of crucial importance in ensuring that human rights abuses do not result from misreported facts or erroneous assessments. In an area where information is always going to be in short supply, open to varying interpretations and often demanding immediate action, the risks of getting it wrong are considerable, as of course are the risks of doing nothing.

The issue of classification is accordingly one that has occupied intelligence services over the ages. A State will classify information according to the damage likely to arise from its unauthorized disclosure.

The damage may be commercial; it may be related to the security of the State; or it may be related to the effectiveness of policy, or the instruments of policy. An intelligence service will take a different approach, classifying its product according to the nature and sensitivity of the source. It may not be terribly important to know what a terrorist leader had for breakfast, but if only his cook has the answer, then the information is by definition highly classified. A third method is to classify information according to the reporting record of the source. Intelligence services and their customers have tried to combine all three criteria by grading sources according to the potential damage to the State, damage to the operation and reliability of the source, the first two referring to the need for protection of the information, the third related to its use.

6. ISSUES ARISING FROM INTELLIGENCE SHARING AND 'ACTION ON'

Not all intelligence that provides identifying particulars of a member of a terrorist group is problem free when it comes to the proper observance of human rights, especially when that intelligence also reveals the person's location. From a human rights point of view, handling this sort of intelligence can be highly problematic in the age of rendition and extra judicial killing. Domestic laws in most countries may be clear on such issues but they are not always in conformity with the laws of other countries. In some jurisdictions, such as currently in the US as a result of the powers conferred upon him by the Authorization for Use of Military Force adopted by Congress in September 2001, the president may order the killing of an individual 'in order to prevent any future acts of international terrorism against the United States',[66] where there is no

[66] See Public Law 107–40, 107th Congress, 18 September 2001, https://www.gpo.gov/fdsys/pkg/PLAW-107publ40/pdf/PLAW-107publ40.pdf, accessed 11 October 2017. The Authorization for the Use of Military Force adopted by Congress on14 September 2001 and signed into law four days later was directed against the planners and perpetrators of the attacks of 9/11. This has governed all subsequent military action against terrorist groups, despite their increasingly tenuous connection with 9/11. In 2015, in order to cover the subsequent and additional threat posed by the so-called Islamic State, the White House proposed that Congress further authorize the limited use of the US armed forces against the Islamic State of Iraq and the Levant. Congress declined to do so.

reasonable prospect of arrest or other means of disruption.[67] This has led to the controversial use of armed drones in third countries, most notably Afghanistan, Pakistan, Somalia and Yemen, whether or not with the agreement of the relevant government.

A problem quickly arises where intelligence gathered by an agency that operates in a jurisdiction where such killing is not legal is passed to an agency that operates in one where it is, potentially exposing the originator to a significant legal liability. Limiting the right to take 'action on' without reference to the originator becomes extremely difficult, especially if the receiving agency believes that the information relates more to its own national security than to the originator's. In the worst case, the originating agency may face a difficult choice of withholding the information at the risk of failing to warn an ally of an impending attack so as to avoid complicity in possible action that might be against domestic law or international human rights law, or risking that transgression in the broader interest of preventing greater harm. Inevitably, by the very nature of intelligence on terrorists and terrorism, it is rare that a piece of information about the location of an individual is also clear about his immediate intentions.

These questions of the moral and legal dilemmas that arise from the ownership and control of intelligence and the right of a subsequent recipient to take 'action on' based on what it reveals have been debated at length, both between and within agencies. Some of the issues have been made public, for example in the report on rendition by the Intelligence Services Committee of the Houses of Parliament in the UK discussed earlier.[68] Realistically, it is not reasonable for any intelligence service providing information to another to have complete confidence that it will only be used in accordance with strictures laid down and assurances given at the time of exchange, especially in matters of life and death. But even where an intelligence service may notify another that one of its nationals is, for example, returning home from fighting with an extremist group abroad, so resulting in his arrest and incarceration under that country's law, if the extremist group is not proscribed by a Security Council resolution adopted under Chapter VII of the UN Charter, there may be disagreement whether such arrest is justified without more process to examine what activities the individual may have been involved in. If however the originating agency does not pass on the information,

---

[67] A White House note of 23 May 2013 sets out the procedures and standards for drone use.

[68] Intelligence and Security Committee (n 53), at 13.

the country of residence of the returning fighter may justifiably complain that the refusal is not in accordance with other Security Council resolutions, such as Security Council resolution 2253 (2015).[69]

Although the international community, including at the level of the Security Council, is increasingly insistent that intelligence on terrorism be shared, leaving aside any operational reasons for not doing so, for example, the risk that the source may be exposed by action taken as a result, there are often very real ethical or even legal issues to take into account as well. No rules can cover all eventualities, and enforcement of whatever rules are agreed will always be subject to the exigencies, interpretations and imperatives of the moment. Moral dilemmas litter the intelligence world, and are not made simpler by the environment in which it spins. Laws governing the collection of intelligence do not generally touch on its use, and for good reason, so leaving crucial questions up to the source, the source handler, their own house rules, and the requirements of the customer. What should be done, for example, if a highly placed source in an active terrorist group is able to provide evidence that would prove beyond doubt the innocence of a man convicted of terrorist acts, but only by exposing himself as an agent of the State, and so losing access to current attack planning and possibly risking his own life and liberty? And who should decide the right course of action in such cases? It may sound hypothetical, but such circumstances are not far-fetched.

7. ISSUES ARISING FROM TECHNICAL INTELLIGENCE OPERATIONS AND THE ROLE OF THE PRIVATE SECTOR

These issues also arise in those forms of intelligence collection that do not involve a human source. Although the revelations in 2013 and subsequently by Edward Snowden, a former US government contractor and employee of the CIA, went far beyond the National Security Agency's (NSA) domestic collection efforts, nonetheless he did initiate a useful debate on the way that the fear of terrorism had led to unauthorized intelligence collection activity that impinged on the individual rights to privacy of US citizens. The bulk collection of data on the basis that it

[69] Security Council resolution 2253 (2015), preliminary para. 29, http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/2253(2015), accessed 11 October 2017.

might be useful in a subsequent investigation would seem not just reasonable but sensible from the point of view of an intelligence agent. The NSA was not acting to undermine the US, but rather to protect it. Nonetheless, the criticism of the NSA and the re-emphasis on its need to act within the law, and, if that seemed insufficient, argue for the law to be changed, were useful reminders that however well motivated and well intentioned any intelligence official may be, in a democracy he is not the one to decide that the interests of the State are better served by contravention rather than observance of the law.

A further debate concerning the interception of communications in the interest of preventing terrorism arises over the issue of encryption. During the latter half of 2015, new features developed for smart phones included a level of peer-to-peer encryption that even major government agencies like NSA could not easily break. The Director of the FBI urged commercial telecommunications companies to ensure that the government was provided a back door into their encryption software, while the tech companies responded that this would give a commercial edge to their non-US rivals and that the government should not demand they take such action voluntarily. It is hard to argue with the tech companies on this score. Highly secure peer-to-peer encryption of communications is now a fact of life, it cannot be uninvented and will presumably become more and more sophisticated as time goes by. Even if the vast majority of users of encryption only seek privacy, rather than to escape the scrutiny of the State, all other things being equal, they would be unlikely to choose a service that allowed the State access to their communications over one that did not. If the US government insists that the communications companies that operate in the US provide a back door to their encryption services, then the US government should introduce legislation that obliges them to do so. This of course would still not solve the problem that bad actors might choose alternative, foreign sources of encryption.

In the aftermath of the attacks in the US of September 2001, the intelligence services of most western countries could tap into a widespread sense of sympathy and obligation among the management of commercial companies that operated within their country's jurisdiction. They could ask informally for help with tracing communication links between suspects, and even revealing information about their clients and the content of their calls. This was true also in the financial world, where intelligence operatives could readily find officials willing to help in support of national counter-terrorism efforts to suppress or investigate the financing of terrorism. The intelligence officials were merely doing their job: recruiting sources with access to the information they required; but

the assumption developed among government officials that anyone who could help should help. This was an extension of the 'either you are with us, or you are with the terrorists' doctrine promulgated by President Bush in his address to a joint Session of Congress on 20 September 2001.[70]

This attitude led to the outsourcing to the private sector of many of the moral and ethical – if not legal – decisions about privacy and proportionality in counter terrorism. But the private sector operates according to commercial decisions, and will maximize its profits insofar as the law allows. Asking a multi-national tech company to provide information voluntarily in one jurisdiction, begs the question as to what it should do with the same request in another, where the authorities may set the 'terrorism' bar considerably lower. In all cases, private companies that are privy to client information that merits protection under specific contract law and by more general rights to privacy, should not be asked to provide intelligence where a refusal to do so might lead to commercial disadvantage. If the government believes that such requests should be met then it should introduce appropriate laws. This then gives the option to both the company and its clients to decide whether or not they wish to do business in such an environment.

8. CONCLUSION

International law recognizes that States may need to recruit informants, conduct sting operations, intercept communications, and deploy electronic surveillance measures. Navi Pillay, the former UN High Commissioner for Human Rights, has acknowledged the vital role that intelligence collection plays in the prevention of terrorist violence: 'The use of accurate intelligence is indispensible to preventing terrorist acts and bringing individuals suspected of terrorist activity to justice'.[71] The Council of Europe's Committee of Experts on Special Investigation Techniques in relation to Acts of Terrorism similarly noted in a report published in 2005: 'The objective of the European Convention on Human Rights is not to disarm the authorities responsible for prevention or prosecution in criminal matters. The Convention sets out criteria in order

[70] See http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html, accessed 11 October 2017.

[71] Report of the United Nations High Commissioner for Human Rights on the protection of human rights and fundamental freedoms while countering terrorism, A/HRC/16/50, para. 33.

that the authorities' activities should constantly be guided by the rule of law and the pursuit of the democratic ideal'.[72]

Not every terrorist attack or national security threat can be prevented, and not every pivotal event can be foreseen. The harsh reality is that when opportunities to prevent attacks are missed, or some game-changing development catches the intelligence community by surprise, this typically reflects a failure of competency, imagination, or capacity on the part of the authorities, rather than any malign restriction or check placed on the intelligence services by the law. Clues that might have enabled the US authorities to disrupt the planning of the September 11 attacks on Washington and New York – most notably the presence of future hijackers Khalid al Mihdhar and Nawaf al Hazmi in the US – were not acted upon in large part because of the stovepiping that characterized the American intelligence community at the time.[73] The chance sightings of the London Transport bombers Mohammed Siddique Khan and Shazad Tanweer in the company of known Islamic extremists were not followed up because MI5 was overwhelmed by what seemed at the time to be more important investigative leads.[74] More intrusive powers would not have prevented either attack and would likely have just generated additional intelligence clutter further obscuring the needle represented by Al Qaeda's activities in a giant haystack of irrelevant data.[75] In the intelligence business less is often more, intelligence driven investigation is efficient; data driven investigation for the most part is not.

The tests set by international human rights law for the use of Special Investigative Techniques go to the heart of the dilemma that faces all intelligence agencies operating within democratic systems – how does one protect the public while also protecting the rights and freedoms they enjoy. There is little point adopting policies that ultimately undermine the institutions they are supposed to protect. As a bumper sticker popular in the US declaims: 'Freedom isn't free'. Some risk is inevitably involved

---

[72] Council of Europe (2005), *Terrorism: Special Investigation Techniques* (Strasbourg: COE), at p. 27.

[73] National Commission on Terrorist Attacks Upon the United States (2004), *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, Authorized Edition (New York: W.W. Norton and Company), at pp. 266–72.

[74] Intelligence and Security Committee (2009), 'Could 7/7 have been prevented? Review of the intelligence on the London terrorist attacks on 7 July 2005', HM Stationery Office, May, paras. 47 and 68–70.

[75] Rosa Brooks (2015), 'The Threat is Already Inside: And nine other truths about terrorism nobody wants to hear', *Foreign Policy*, 20 November.

living in a free society. The challenge is to get the balance right, to ensure, in the words of the current Director General of MI5, Andrew Parker, that being on the authorities' radar is not the same as being under their microscope.[76] Intelligence officers are a country's first line of defense and international human rights law provides an effective framework within which to operate. An intelligence service that loses touch with that reality may ultimately pose a bigger threat to the society it is seeking to protect, than any terrorist group or foreign power.

[76] Address by the Director General of the Security Service, Andrew Parker, to the Royal United Services Institute (RUSI), Whitehall, 8 October 2013.