Transatlantic intelligence and security cooperation

RICHARD J. ALDRICH*

Transatlantic intelligence and security cooperation appear to have been considerably enhanced over the past three years. Both intra-European and EU–US intelligence cooperation were substantially expanded in the wake of 9/11.[1] Most visibly, Operation Eagle Assist provided additional European AWACS aircraft to protect the United States, releasing American aircraft for duty elsewhere;[2] and in late September 2001 Europol, a relatively young institution, was designated a central point for data exchange between European law enforcement agencies and the United States.[3] More recently, prompted by the bomb attack on Madrid earlier in the month, the EU summit of 25–26 March 2004 agreed on a Europe-wide security coordinator and Gijs de Vries was appointed to this new post under Javier Solana.[4]

Such appearances of closer cooperation, however, are only superficial; at a more fundamental level, significant problems remain. Concerted efforts to improve intelligence exchange on terrorism have been in train since the 1970s. Indeed, some have argued that substantial western intelligence cooperation—often referred to as liaison—has its roots in nineteenth-century efforts to

---

1 On this subject see N. Bensahel, *The counterterror coalitions: cooperation with Europe, NATO, and the European Union* (Santa Monica: RAND Project Air Force, 2003); Glen Segell, 'Intelligence agency relations between the European Union and the U.S.', *International Journal of Intelligence and CounterIntelligence* 17: 1, Spring 2004, pp. 81–96. The classic functional analysis of intelligence liaison is Bradford Westerfield, 'America and the world of liaison', *Intelligence and National Security* 11: 3, July 1996, pp. 523–60.
2 NATO press statement by Secretary General, Lord Robertson, on the decision to implement Article 5, 4 Oct. 2001.
3 Rory Watkins, 'Anti-terror chief little known outside Brussels', *The Times*, 27 March 2004.
4 They are scheduled to report to the European Council on improved intelligence cooperation in the summer of 2004. See summary transcript of joint press briefing by Javier Solana, EU High Representative for the CFSP, and Gijs de Vries, Counterterrorism co-ordinator, 30 March 2004, Brussels, at http://ue.eu.int/pressData/en/declarations/79752.pdf.

exchange information on Sikh, Fenian and anarchist groups that were committed to violence.[5] Yet despite decades of joint activity, transatlantic intelligence cooperation continues to present awkward challenges. These problems have become more substantial with NATO enlargement and EU expansion.

The traumatic events of 11 March 2004 in Madrid underlined the opportunities offered to terrorists and criminals by hesitant or partial intelligence exchange. Some of the suspects in the Madrid bombing had been of interest to the French and Spanish police in 2001 but had been released for lack of evidence. By 2003, two of them were on a list of suspects issued by the Moroccan police for a series of café bombings in Casablanca, but were nevertheless living openly in Madrid. Retrospective investigation has turned up further information on their connections in Germany and Norway. Each country seemed to have a few pieces of a widely spread puzzle.[6] More remarkably, during early April 2004, the inability of the United States to provide Germany with access to a member of Al-Qaeda arrested in Pakistan and held by the US at an undisclosed location, contributed to the early release of Mounir el-Motassadeq, an important suspect who was before the courts in Hamburg on charges relating to the 9/11 attack.[7]

Intelligence and security cooperation continues to be problematic because there is a fundamental tension between an increasingly networked world, which is ideal terrain for the new religious terrorism, and highly compartmentalized national intelligence-gathering. The networked world is a well-known (or at least well-recognized) aspect of globalization. Compartmentalized national intelligence-gathering is less well understood. Compartmentalization occurs for two reasons. First, western secret services rightly place a high premium on protecting their sources. Second, western states have different notions of privacy and so resist large-scale data-sharing. Source-protection is such a firmly established convention that it is unlikely to change; as a consequence, secret services will not move towards sharing high-grade 'killer punch' intelligence material on anything but a selective and bilateral basis. However, more routine background intelligence must be shared at a faster rate, and to achieve that we require a better joint understanding about the relationship between privacy and security. In particular we will need improved benchmarks regarding what sort of intelligence should be shared and how it will be managed. Developing an improved conceptual framework within which to tackle the necessary trade-offs between security and privacy is essential for closer transatlantic cooperation.

[5] C. M. Andrew, *The growth of intelligence cooperation in the English speaking world*, Wilson Center Working Paper no. 83, Nov. 1987; R. J. Popplewell, *Intelligence and imperial defence: British intelligence and the defence of the Indian empire, 1904–1924* (London: Frank Cass, 1995), pp. 147–64.

[6] Peter Finn and Keith B. Richburg, 'Madrid probe turns to Islamic cell in Morocco', *Washington Post*, 20 March 2004; J. Lichfield, E. Nash, S. Castle and J. Bennetto, 'Europe must share terror intelligence', *Independent*, 17 March 2004.

[7] 'Jailed Sept. 11 plotter released pending re-trial', *Washington Post*, 7 April 2004; 'World's only 9/11 convict released due to US non-co-operation', *Wall Street Journal*, 9 April 2004.

The mismatch between the narrow national focus of recent inquiries into intelligence-related episodes and the growing importance of multinational cooperation has further clouded our understanding in this area. The 9/11 Commission has probed bureaucratic divisions within the United States only. In the UK, the Hutton inquiry enjoyed an even narrower remit. The same has been true of lower-profile reviews in countries as diverse as Denmark and Australia.[8] Arguably, because of the networked nature of the new threats, the primary concern should be weaknesses in international cooperation, not in national structures. The good news is that cooperation is possible, even between countries that do not like each other and even at times when transatlantic tensions are high. The better news is that new forms of cooperation are emerging, particularly among the countries of Europe. The primary lesson here is that the focus needs to be on speeding up means of practical exchange on operational matters, not on building elaborate new structures. Ultimately, the politics of intelligence is a practical one, with a 'pay as you go' culture in which the main producers will not relinquish their accustomed dominance to new multilateral organizations set up by the EU—or by anyone else.

Many transatlantic institutions were created during the Cold War at a time when international events moved more slowly. Accordingly, neither NATO nor the EU is accustomed to acting with the speed required by effective counter-terrorism operations. Expansion and enlargement will render these bodies even more cumbersome. Nevertheless, as this article suggests, the EU has important contributions to make at the level of law enforcement and improved security, while NATO is taking significant strides at the level of military intelligence cooperation with new members. Moreover, the sense of urgency generated by the bombings in Istanbul and Madrid is accelerating measures that will have important consequences for wider transatlantic intelligence cooperation against drugs, organized crime, people trafficking and other security threats.[9]

Intelligence and security services, as their name implies, are designed to provide a supporting 'service' to other operational and policy mechanisms; and indeed, transatlantic intelligence and security cooperation connects with almost every aspect of the western alliance. However, in the past three years it is, specifically, terrorism that has exercised a transformative effect on this area, and accordingly the focus here is on efforts to respond to that challenge. The article begins by seeking to advance a more nuanced understanding of the trade-offs between security and liberty that might be applied to new provisions for data retention or exchange within the NATO alliance. Thereafter it proceeds sequentially, asserting that these provisions will apply differently across three distinct types of intelligence activity. The secret services are primarily focused

---

[8] Although the issue is not explored in this paper, one effect of the increasing numbers of multinational intelligence operations, often with an exotic range of partners, is the inability of national mechanisms for accountability and oversight to examine them.

[9] On the important development of the EU as an internal security actor across issues of justice, crime and illegal immigration see V. Mitsilegas, J. Monar and W. Rees, *The European Union and internal security: guardian of the people?* (London: Palgrave, 2003).

on prevention and counteraction; therefore the material that they share is unlikely to arrive in the public domain, or manifest itself in court proceedings. By contrast, police intelligence, telecom data and passenger records present problems associated with wider access and judicial implications. Military intelligence is different again, although this too is increasingly harnessed to the wheel of counterterrorist interventions. The article suggests that almost all the problems of intelligence exchange in these three areas are resolvable. However, the challenge of arriving at a joint agreement as to what the shared intelligence means in broad terms is more problematic. Although some prominent commentators have suggested that shared NATO strategic intelligence estimates would enhance alliance cohesion, the last section of this article argues that they would be difficult to achieve and of doubtful effectiveness.

Security, privacy and anonymity

The most serious challenge confronting transatlantic intelligence cooperation is identifying an appropriate fulcrum that allows us to continue to balance security and liberty. Gijs de Vries has characterized this problem as improving security while respecting fundamental freedoms. He has avowed his intention not only to preserve European liberties but also to find a way to build upon them. These are fine words, but the practice is likely to be difficult. As Michael McDowell, the Irish justice minister, has conceded, security pressures will require access to more data by an ever wider range of security officials. If reluctance to share intelligence contributes to serious security failures, the public will be highly intolerant of those who obstructed a free flow of data.[10]

Although the legal bases for the regulation of both intelligence and privacy in Europe and the United States are different, there are significant points of commonality. The most important is the idea of 'proportionality'. Whether an instance of proposed surveillance is assessed by a middle manager in Whitehall, or whether a request is being made before a Foreign Intelligence Surveillance Court in Washington, the underlying principle dictates that the degree of intrusion be kept proportionate to the threat confronting the civil population. Although sometimes applied imperfectly, this framework has served democratic states on both sides of the Atlantic as a benchmark for many years. In Europe, the growing incorporation of ECHR provisions has only served to strengthen this principle. However, proportionality is now an increasingly difficult concept to apply in the face of a new kind of terror, which has no upper limit. In the face of the threat of a strategic terrorist attack the difficult question to answer is, how much surveillance is enough?[11]

---

[10] Ian Black, 'The European dilemma: the Madrid bombings are shifting the balance between civil liberties and security', *Guardian*, 2 April 2004.

[11] In the US the Foreign Intelligence Surveillance Act of 1978 set up a special review court in Washington DC and standardized a proportionality test (that the benefits of surveillance outweigh the harms). It also required an 'exhaustion test' to show that more conventional investigatory methods had failed. UK regulations based on Article 8 of the European Convention on Human Rights are framed in a similar way.

It is improbable, and indeed unfair, to expect the intelligence and security services to resolve these difficulties. Such choices are not matters for security chiefs, or even for ministers: they are matters of social choice and require serious and extended public debate. The idea of proportionality remains important and will continue to offer a benchmark for intelligence services' operational activities for the foreseeable future. Proportionality is bolstered by the test of 'necessity', or whether the same information can be secured by more innocuous means. Institutional capacity often imposes additional and very practical restraints in a business which is resource-intensive. However, at a more strategic level none of these ideas offers the policy-makers much guidance as they attempt to make their way through the labyrinthine maze of intelligence alliances and international data-sharing arrangements. What material should be shared and how freely? And where might we look for additional signposts to guide policy-makers?

One of the problems that has bedevilled thinking about the balance between security and liberty has been weak definition. In particular, public debate over new security measures has tended to confuse the distinct subjects of secrecy, privacy and anonymity. If the transatlantic community is to protect core freedoms and essential civil rights it needs a more sophisticated understanding of what we are attempting to protect. Historical sociologists would be quick to point out that ideas concerning state security mechanisms belong to particular epochs no less than those relating to military strategy. We currently enjoy a range of security mechanisms inherited from the Cold War, and these must be reshaped to address new problems set against the background of globalization. Accordingly, we could do worse than to consider how successive conceptions of secrecy, privacy and anonymity have changed over time. Protests against new counterterrorist measures are frequently advanced on the basis that the tariff for more security is an unacceptable degrading of our freedoms. However, a longer-term perspective would allow us to be more discerning in our approach, selecting measures which do not significantly erode core privacy but which are designed to reduce the dangers of anonymity.[12]

In the pre-industrial era, the majority of human beings lived in villages. Set within this largely rural landscape, citizens enjoyed privacy but not anonymity. Activities within their own domestic sphere were largely invisible to their neighbours, but as they went about their business they were known to their community and their purpose was understood. Strangers entering a village were quickly identified and, in a civil way, the nature of their business was established. Although it is easy to exaggerate the bucolic innocence of this rural idyll, the important point in the present context was that there was little anonymity, and if a crime was committed, the identity of the perpetrator was often known to some section of the community. However, industrialization radically changed this pattern. Industrialists desired the free movement of

---

[12] American civil liberties groups were in fact rather slow to react to the Patriot Act of 2001 and are only now mounting substantial legal challenges to some its provisions.

landless labour while the authorities feared mobile populations. The pressures of attendant urbanization upon the domestic sphere eroded privacy, while extending vast anonymity in the form of the faceless urban crowd, wherein those of ill intent could cloak themselves. Although states responded with police forces, the introduction of passports and fingerprinting, these measures moved at a constabulary pace and industrialization was usually more than one step ahead.[13]

In the twenty-first century, globalization continues to accelerate this process. In common parlance we often refer to the information revolution as shrinking time and distance and so creating something that we are pleased to refer to as the 'global village'. However, globalization has not delivered a 'global village'. Instead it has produced a global mega-metropolis in which there is vast anonymity and diminished privacy. Our new security regimes and the way in which we share data must be carefully configured to reverse this trend. Attainment of anything like a global village is still far away from us, but the instinctive attractiveness of this term perhaps points the way ahead, towards a place where privacy is better preserved, while the scale of anonymity is reduced.[14]

Knowing who someone is, why they are in a particular public space and what their business is does not require intrusive surveillance. Knowing what their religious affiliation is, what food they prefer, what their bank balance is and what they said to their spouse on the telephone last week is, by contrast, much more invasive and trespasses upon their privacy. Although privacy is a curiously existential concept, nevertheless the preservation of the boundary between the public and the private is at the core of what defines the liberal state. Many of the new security measures under consideration across Europe and North America, including biometric passports, will not erode privacy, but they will curtail dangerous anonymity and protect individuals from the unpleasant practice of identity theft. By contrast, other measures, such as those that involve the transfer or agglomeration of large amounts of personal information from many different databases, including commercial sources, constitute a more substantial threat to privacy.

We need to keep these distinctions in mind. Judicious use of information technology, together with discriminating and sensible patterns of intelligence cooperation, will take us a long way in our efforts to protect transatlantic society. In other words, if we can get this right, the activities of security and intelligence organizations need not erode the qualities of freedom in a democracy; instead they can sustain and extend our liberties.

---

[13] J. Torpey, *The invention of passport surveillance, citizenship and the state* (New York and Cambridge: Cambridge University Press, 2002).

[14] These distinctions between anonymity and privacy draw in part on the Detweilerian thesis on nymity that asserts that human interactions based on honest formal identification systems enjoy a superior quality.

Secret intelligence and the civilian agencies

The leading elements in the effort to counter terrorism are the most secret. These are the civilian intelligence and security services of the larger states in North America and Europe. In this domain the overwhelming emphasis is upon tight security for information being exchanged, and this is not unhelpful in our search for enhanced privacy. Intelligence exchange between these organizations is a world within a world, governed by its own diplomacy and characterized by elaborate agreements, understandings and treaties. The main substance of these agreements focuses upon the security of intelligence rather than intelligence exchange itself, and reflects concern over how that intelligence will be circulated within each national system. This, in turn, fosters an attitude of intense caution towards the idea of sharing, and especially towards multilateral sharing. Moreover, in Europe and the United States, secret services are often close to the core executive and so associated with ideas of sovereignty. States will happily place some of their military forces under allied command, but hesitate to act similarly in the area of intelligence, where coordination rather than control is the most they will accept. This resistance to the multilateral pooling of very sensitive data, on security grounds and wider concerns about sovereignty, will prevent both an unhealthy agglomeration of secret data and the rise of a federal super secret service. What we are seeing instead is a focused effort to cooperate more quickly on specific cases or to exchange limited data more effectively.

The most remarkable example of cooperation is the English-speaking effort in the realm of signals intelligence (sigint) known as UKUSA.[15] Sharing in this realm between the United States, the UK, Australia and Canada is so complete that national product is often indistinguishable. But this is an Anglo–Saxon rather than a transatlantic partnership; moreover, the institutional linkage between UKUSA and continental European states has diminished, rather than grown, over the last decade. The United States has withdrawn some sigint assets from Germany and relocated them within the UK. The Dutch have advocated a stronger national sigint capability after a disappointing experience with multinational sharing in the Balkans.[16] The French have attempted to interest other European states in serious investment in a parallel European system for both sigint and satellite imagery, but without success. With no one to share the mounting costs, Paris was recently forced to cancel its Zenon sigint satellite programme.[17] London remains firmly oriented towards the United States, in part because it provides the UK with intelligence as a 'loss leader'; there is a recognition in Washington that this removes the attraction of alternative Europeanist ventures. The sigint agencies do not have a monopoly

---

[15] C. M. Andrew, 'The making of the Anglo-American SIGINT alliance', in H. B. Peake and S. Halpern, eds, *In the name of intelligence: essays in honor of Walter Pforzheimer* (Washington DC: NIBC Press, 1994), pp. 95–109.

[16] Menno Stekee, 'Major General Bert Dedden', *Jane's Intelligence Review*, 1 Dec. 2003.

[17] J. Guisnel, 'Espionnage: les français aussi écoutent leurs alliés', *Le Point*, 6 June 1998.

on technical interception. Security services also play a growing role, focusing on e-mail; and here too, the sharing of sensitive intelligence remains largely a UK–US affair. The sheer scale of the apparatus employed by the United States explains why the United States remains the most important bilateral partner for the UK's Security Service.[18]

Unsurprisingly, intelligence cooperation is partly about building confidence, and the time-line is necessarily long. Western security services have been developing their associations for decades and these are now growing in importance. These security networks exchange less sensitive data, background studies, scenario analyses and policy views. As early as the 1960s the English-speaking countries began a compartmentalized security alliance called 'CAZAB' that searched for evidence of high-level Soviet penetration. In the 1970s a wider group of countries began two intelligence-sharing systems on Middle Eastern terrorism codenamed 'Kilowatt' and 'Megaton'.[19] But perhaps the most enduring of these arrangements has been Europe's Berne Group, formed in 1971 and sometimes called the 'Club of Berne'. Initially consisting of only six European security agencies, including the UK's Security Service, the French DST, the German BfV and the Swedish SÄPO, it now numbers 17 members, the most recent adherent being Greece. This is more than a lunch club: the heads of the services meet twice a year for formal security summits. The Berne Group has it own communications network administered by the UK and several working groups on subjects such as terrorism, organized crime and interception. These are also joint training courses for younger staff. All this joint activity contributes to a further vital function, the building of mutual confidence and trust.[20]

Little publicity has been given to successful European security intelligence cooperation immediately preceding 9/11. In early 2001 intelligence indicators suggested that Osama bin Laden was planning a campaign of bomb attacks in Europe. Based on a 'well-functioning international exchange of information' among the major security and intelligence services in Europe, a number of successful operations against persons within the bin Laden network were launched. By mid-April 2001, a total of eighteen individuals had been appre-hended in a series of coordinated operations across Europe. During some of these, weapons and chemicals intended for the manufacture of explosives were seized. In other words, the long-established Berne Group was functioning fairly well.[21]

---

[18] The UK Security Service helps to operate an e-mail decryption facility called the National Technical Assistance Centre (NTAC).

[19] They involved the usual transatlantic partners together with countries as diverse as Norway, Israel and South Africa. I am indebted to Philip Gregory of St Peter's College, Oxford for information on this subject.

[20] The Berne Group consists of 17 member states with representatives from 19 organizations. This draws in part on the Hinsley Lecture 2003, given at the University of Cambridge by Sir Stephen Lander, 'International intelligence cooperation: a modern perspective', forthcoming in *Cambridge Review of International Affairs* 2004.

[21] Annual Report of SÄPO (Swedish Security Service) 2001, http://W.security service.se/ Publikationer.annuak_01.doc.

However, successful as it may be, the Berne Group is not transatlantic and the United States is not a member. Accordingly, following 9/11 the Berne Group created a new organization called the Counterterrorist Group (CTG). This is a separate body with a wider membership of EU intelligence and security services, together with the United States, Switzerland and Norway.[22] The first meeting was held in November 2001 at The Hague, chaired by the Belgian security service. The main current product of this group is common threat assessments in the field of Islamic terrorism. Although CTG is not an EU organization and reports through national security services to each capital, nevertheless the national chair of CTG rotates in synchronization with the EU presidency and its threat analyses are made available to some high-level EU committees. During 2002 and 2003 CTG devoted considerable energy to institutional matters and the problems of multilateral data exchange. CTG does not have a geographical headquarters, but is probably the most important focus of day-to-day cooperation. Current CTG discussions point towards a shared database within the next five years. This would not contain sensitive material, but would allow the collation of contextual intelligence on suspects. At its most recent meeting in Switzerland on 21 April 2004, the Berne Group decided that CTG should play the major role in implementing intelligence-related aspects of the European Council's Declaration on Combating Terrorism that followed the attack on Madrid.[23]

The new members of the EU and NATO render this picture more complex. Relations with the 'new Europe' have been handled through the Middle Europe Conference, a different collaborative network run by a number of West and Central European security services. This was set up at the suggestion of the Dutch security service in 1994 and played a long-term preparatory role in the accession to the EU in 2004 of ten new countries.[24] Its focus has been on accountability, political control and the role of security services in support of democratization rather than counterterrorism. It has also provided a useful forum for discussing issues relating to organized crime. On 1 May 2004 these ten countries joined CTG as full members.[25]

Although some countries, notably Belgium and Austria, have recently made public calls for the creation of a Europe-wide FBI, EU expansion makes these improbable ambitions even more unlikely to be realized. Such proposals have for the most part come from states that have a limited national security intelligence capability and now feel vulnerable.[26] Capability is everything in the

---

[22] Technically the United States has observer status in CTG.

[23] Politiets Efterretningstjeneste (PET) [Danish Security Intelligence Service], 'Samarbejdspartnere', http://www.pet.dk/Samarbejdspartnere.aspx.; Swiss Federal Office of Police press release, 'Club de Berne meeting in Switzerland', 28 April 2004, http://internet.bap.admin.ch/e/aktuell/index.htm.

[24] In 2002 the Czech Security Information Service (BIS) joined the Middle European Conference's Evaluation Committee, which is focused on these issues: BIS Annual Report 2001, sec. 8, 'Cooperation with intelligence services of foreign powers', http://www.bis.cz/_english/info_.html.

[25] Annual Report of the Dutch General Intelligence and Security Service (AIVD) 2002, pp. 61–3, http://www.aivd.nl/actueel_publicaties/publicaties/annual_report_2002.

[26] Guy Verhofstadt, the Belgian prime minister, has been prominent in calling for a European intelligence service: R. Minder, 'EU justice ministers to hold "terror" meeting', *Financial Times*, 16 March 2004.

world of intelligence and all the pre-existing networks have their places in an established hierarchy. There is more competition than cohesion, with big producers dominating the networks and small producers remaining on the periphery. The major players, including the UK, like it this way, and so little will change. Typically, on 31 March 2004 the UK minister of state for Europe, Denis MacShane, emphasized that any EU-based intelligence activity should be limited to 'producing assessments at a more strategic level', adding that the real work can 'only be done within a national framework'. There would be more sharing of assessments, but ministers were 'not acting to set up any kind of European intelligence agency in any way'.[27]

Publicly, Gijs de Vries has taken a similar line, portraying himself as a facilitator of cooperation rather than someone who is seeking to create bold new frameworks.[28] Privately, the EU has long nurtured ambitions to expand its intelligence capability because this is the logical corollary of a common foreign and security policy. Recent efforts have been focused on the Joint Situation Centre or 'Sitcen'. This is an analytical element that supports 'Second Pillar' or foreign policy activities. Its stated purpose is to provide early warning and conflict prevention information, with a focus on issues outside the EU.[29] However, de Vries has now suggested that its capabilities need to be extended to the analysis of internal security issues, which are now inseparably linked to foreign policy. In early 2002 the Western European Union satellite centre near Madrid and an analytical centre, the Institute for Security Studies (ISS), in Paris were transferred to EU supervision. In January 2004 ISS produced a paper advocating the further enhancement of European intelligence, focused on Sitcen. Currently, the focus on building up Sitcen is mostly about political symbolism and reassuring public opinion that Europe is working together to avert future terrorist attacks.[30]

Liaison between European security services and the United States remains problematic.[31] In the wake of 9/11 a large number of FBI agents arrived in Germany and began independent investigations, to the chagrin of their German hosts. There are now almost as many FBI as CIA personnel in Europe. The French have displayed sensitivity about the FBI's interest in extending its influence in Eastern Europe through its International Law Enforcement Academy in Bucharest, interpreting this as encroachment into Europe's

---

[27] HC 511I, minutes of oral evidence taken before the House of Commons European Scrutiny Committee, 31 March 2004, Q38.

[28] Perhaps de Vries's most important credential is not his background as a deputy home affairs minister or his reputation as an effective European technocrat, but his obvious commitment to transatlanticism. He chaired the Atlantic Commission from 1991 to 1997; and he has dual Dutch and American citizenship, having been born in New York. Thomas Fuller, 'Dutchman could fill terror post', *International Herald Tribune*, 25 March 2004.

[29] O. R. Villadsen, 'Prospects for a European common intelligence policy', *Studies in Intelligence* 9, Summer 2000, http://www.cia.gov/csi/studies/summer00/art07.html.

[30] B. Muller-Wille, *For our eyes only: shaping an intelligence community within the EU*, Institute of Strategic Studies occasional paper no. 50, Jan. 2004.

[31] 'Critics inside intelligence community say that post 9/11, agencies still not sharing intel', *Newsweek,* 28 March 2004.

backyard.[32] Each country has its own peculiarities. Germany finds sharing security intelligence difficult because of awkward constitutional limitations and its federal structure. France has been beset by internal infighting between its own secret services. These complexities translate into myriad complex interfaces with the many competing American agencies located around Washington's beltway.[33]

The American intelligence community has long been noted for its lack of communal identity. Ingrained reluctance to share, together with incompatible data systems, was a key factor in explaining intelligence problems preceding 9/11. Washington has sought to counter this problem by the establishment of the Terrorist Threat Integration Centre (TTIC). Created in May 2003 to remedy the failure of US intelligence and law-enforcement agencies to communicate, the TTIC is an analytical centre tasked with collating data from more than a dozen American intelligence agencies and since June 2004 has enjoyed its own independent headquarters in Washington DC. However, the CIA retains it own rival Counterterrorism Center, while the Pentagon likes neither. The overwhelming pathologies within the American system remain the lack of an overall intelligence director who controls (rather than coordinates), the predominance of the military and the lack of an effective internal security service. These difficulties make liaison more difficult and none of them is likely to be resolved in the medium term. Perhaps they will eventually be addressed only in the wake of another major attack.

Intelligence and law enforcement

Intelligence gathered by police and customs officials represents a different realm wherein the focus is often investigation of crimes after they have occurred. Since the early 1990s both the EU and the United States have been engaged in a prolonged, complex and somewhat sluggish programme of cooperation aimed at tightening financial regulations, standardizing procedures for arrest and improving data exchange. Within Europe efforts have focused on the so-called 'Third Pillar' areas of justice and home affairs. Many supposedly 'new' security measures, whether national, European or transatlantic in scope, had been sitting around on the desks of security officials for a long time before 9/11. Ministers had been reluctant to take them forward until the new climate of emergency provided them with opportunities. Even in 2001, many of the EU measures taken against terrorism were framework decisions that did not require all member states to comply immediately; however, in March 2004 the process of compliance was dramatically accelerated.[34]

---

[32] W. Rees, 'Justice and internal security', in J. Peterson and M. A. Pollack, eds, *Europe, America, Bush: transatlantic relations in the twenty-first century* (London: Routledge, 2003), pp. 56–7.

[33] Within the UK, cooperation has been enhanced by the creation of the Joint Terrorism Analysis Centre (JTAC), located at Thames House. On longstanding issues of intrastate liaison within the United States see J. J. Wirtz, 'Constraints on intelligence collaboration: the domestic dimension', *International Journal of Intelligence and Counterintelligence* 6: 1, Spring 1993, pp. 85–99.

[34] On these measures see M. Den Boer and J. Monar, '11 Sept. and the challenge of global terrorism to the EU as a security actor', *Journal of Common Market Studies* 40, 2002, pp. 11–28; D. Dubios, 'The attacks of

The kind of intelligence that relates to law enforcement issues often appears pedestrian alongside some of the secret service activities discussed above; however, it cannot be overemphasized that dutiful collection and exchange of rather mundane data, sometimes merely open data such as names and addresses, often produces important results. In the 1970s, an Italian decision to enforce civil regulations requiring landlords to notify the authorities of the names of their tenants—an existing but neglected requirement—turned up many of the terrorist suspects currently being sought. At this level there are fewer problems with secrecy and source protection, but greater constitutional sensitivities, not least because some of the information transferred may end up being used against defendants in court. Moreover, names and addresses are one thing; private information is quite another. Some of the most recent EU–US agreements have permitted too much access to personal data by categories of officials that are extremely widely defined. This is a substantial threat to privacy that points to future trouble.

Perhaps wrongly, public attention has been drawn to new institutions and focused upon Europol, an organization set up in 1995 to enhance European police cooperation.[35] Immediately after 9/11 a new counterterrorism unit was announced at Europol, to which many European states dispatched additional security liaison officers. At the same time Europol was designated the key point for the exchange of police intelligence data with the United States. By 6 December 2001 a grandly entitled 'Strategic Cooperation Agreement' had been reached between the United States and Europe, and by the summer of 2002 a liaison team of Europol officers was ensconced in the EU's offices in Washington.[36] However, Europol is a small organization and is often misunderstood. Set up to facilitate police cooperation between two or more willing partner states in particular investigations, it is not to be mistaken for an EU criminal intelligence agency. It has undertaken excellent work against drug-trafficking and people-smuggling, but Europol officials privately concede that a coherent anti-terror policy is beyond both its remit and its resources.[37] It also found European secret services reluctant to offer them information in anything but a sanitized form, and so eventually its counterterrorism unit was reabsorbed into the more mainstream Organized Crime Department.[38]

---

11 September: EU–US cooperation against terrorism in the field of justice and home affairs', *European Foreign Affairs Review* 7: 3, 2002, pp. 317–35.

[35] Europol's mandate was expanded in 1998, 1999, 2000 and 2001: see J. D. Ochipinti, *The politics of EU police cooperation* (Boulder: Lynne Rienner, 2003).

[36] On Europol and the US see esp. Rees, 'Justice and internal security', pp. 47–58; Segell, 'Intelligence agency relations', pp. 82–3.

[37] Europol has developed machine translation for drugs intelligence in cooperation with various European software firms and with assistance from the German BND: EU-Projekt Aventinus, http:// svenska.gu.se/aventinus/.

[38] In 1999 a Belgian official involved in the SIRENE network (an adjunct to the Schengen Information System) sold data to criminals: House of Lords, European Communities Committee, minutes of evidence, 13 Jan. 1999, p. 156, http://www.parliament.the-stationery-office.co.uk/pa/ld199899/ ldselect/ldeucom/37/9011302.htm.

Much more important were the difficult negotiations with the United States over the exchange of personal data held by Europol. The transfer of police data is a legal minefield because of the very different structures of protection accorded to personal information in the United States, where the issue is one of legal precedent, and in Europe, where there are draconian data protection laws. Hitherto these differences have made the sharing of personal data almost impossible. Alex Türk, the EU data protection commissioner, led a team from the joint supervisory body of Europol that attempted to tackle this awkward issue. Their difficulties were compounded by the recognition that it would be unconstitutional for European officials to transfer data that might contribute to the use of the death penalty in the United States.[39] In December 2002 an EU–US agreement was reached; but, based on weak and ad hoc reassurances offered on a case-by-case basis, it is arguably highly problematic on several counts. Its provisions allow exchange of data on any offence; it allows the data to be provided to even local US authorities; and the restrictions on passing data on to third parties are weak. Most problematic of all, the categories of data include race, religious/political opinions and health information. In the UK, the House of Lords expressed alarm but the UK government chose to override its scrutiny process.[40] Less well publicized was a similar package negotiated at the tenth EU–Russia summit on 11 November 2002, which included an information exchange agreement between Europol and the Russian security authorities.[41]

Equally problematic are draconian measures designed to give EU law-enforcement officials access to computerized booking information held on travellers. Again, this includes sensitive personal data such as payment information, bank numbers, credit card data—even food preferences. This will allow the Europe-wide circulation of data that the EU had already agreed to hand over to US security agencies under agreements associated with airline passengers. Large neural network computers that use algorithmic data-mining in an attempt to spot suspicious events are notoriously hungry for these kinds of personal data.[42] Transport information also spotlights another significant aspect of transatlantic intelligence-sharing. In a growing climate of commercial data surveillance (now dignified with its own neologism as 'dataveillance') much critical information is held by companies, such as airlines, rather than states. Trying to persuade United Airlines, British Airways and Air France to share commercially sensitive data about their customers was almost as difficult as national intelligence-sharing.[43]

---

[39] In 2001 a similar problem had hampered exchanges between the German authorities and the FBI over the case of the alleged '20th hijacker' and French citizen, Zacarias Moussaoui.

[40] For a cogent review of these issues see V. Mitsilegas, 'The new EU–USA cooperation on extradition, mutual legal assistance and the exchange of police data', *European Foreign Affairs Review* 8: 4, Winter 2003, pp. 515–36.

[41] EU–Russia joint statement on the fight against terrorism, 11 Nov. 2002, http://europa.eu.int/comm/external_relations/russia/summit_11_02/js_terr.htm.

[42] The important subject of data-mining, especially using commercial databases, has largely been overlooked, but see M. de Rosa, 'Privacy in the age of terror', *Washington Quarterly* 26: 3, Summer 2003, pp. 27–41.

[43] S. K. Goo, 'EU agrees to share airline passenger data', *Washington Post*, 17 Dec. 2003.

Cooperation in tracking the financing of terrorism has been placed high on the agenda within both the EU and the UN.[44] This priority resulted in a series of measures to freeze the assets of terrorist organizations. Within the EU the operational activities are undertaken by a small working group, based in Brussels, in bilateral cooperation with member states. Despite the creation of new frameworks for cooperation and better electronic databases of targeted persons, this work remains complex, detailed and slow. Although officials have worked hard in this area, the instruments remain unequal to the task. The fundamental framework remains the Financial Action Task Force set up by the G7 in 1989, which ideally should be replaced by a properly resourced international organization. There are already signs that suspects are moving towards informal financial transfers that will deny investigators valuable paper trails in the future.[45]

Current EU proposals seek to retain telecommunications data, including records of mobile phone traffic, in all member states for an agreed minimum time to enable intelligence agencies to track calls. Although this has been controversial, it does not in fact involve holding transcripts or recordings of messages, but merely preserving caller information (although the two are linked in that some mobile telephone records can give the timed geographical location of callers). Currently, this area is beset by discrepancies. Sweden obliges its telecom companies to keep such records for only three months, the UK for one year, France for three years and Italy for five years. Other practical security cooperation measures which have yet to be implemented include the European common arrest warrant, whose enforceable provisions await enactment in Germany, Italy, Greece, Austria and the Netherlands. The EU-wide definition of terrorism has not yet been adopted by three member states, which have been urged to set out minimum sentences for terrorist crimes.[46]

In the longer term, the most important EU measure under discussion is the plan for a high-tech ID database using digital 'biometric' technology. The proposals before EU justice ministers include embedding EU identity documents with microchips containing digitized photographs and fingerprints. In practice this will entail fingerprinting for all EU citizens and the holding of these data on an EU database allowing the tracking of individuals. Dramatic as it may seem, this does not represent a substantial invasion of privacy and deserves to be given high priority. Significantly, this is not only an EU programme. The UK home secretary recently remarked that policy on identification cards and a database with biometrics was 'part of the wider discussions which … are taking place with the G8 countries'.[47] The primary focus is not advancing surveillance but

---

[44] J. L. Hirsch, *The UN and international terrorism*, International Peace Academy Report, 2004; C. de Jonge Oudrat, 'Combatting terrorism', *Washington Quarterly* 26: 4, Fall 2003, pp. 163–76.

[45] Magnus Ranstorp with Jeffrey Cozzens, 'The European terror challenge', 25 March 2004, http://news.bbc.co.uk/1/hi/world/europe/3563713.stm.

[46] 'New counterterrorist measures for Europe', *The Times*, 25 March 2004; memo/04/66, 'European Commission action paper in response to the terrorist attacks on Madrid', Brussels, 18 March 2004, http://europe.eu.int/rapid.start.cgi.guesten.ksh?p_actiongettxt=gt&doc=M.

[47] David Blunkett, minutes of evidence given before the House of Commons Defence and Home Affairs Committees, 2 March 2004, Q43.

merely regaining reasonable control of borders. Together with electronic border surveillance equipment, and CCTV and electronic data collection at air and seaports, these measures will allow the state to reclaim some lost ground and redress the balance somewhat in the face of increasingly mobile populations.

Military intelligence and alliance capability

Defence is one area where divergent alliance policies and priorities have a direct impact on the potential for intelligence cooperation. The United States sees military intervention as the dominant component of the war against terror and intelligence spending focused on supporting defence activity accordingly remains at the forefront of the American effort; European approaches are rather different. This divergence is not a new phenomenon and continues a trend visible throughout the 1990s. It is commonplace to remark that the United States is now engaged in a programme of military spending that is broadly equivalent to that of the rest of the developed world put together. Much of this spending is directed towards 'Joint Vision 2020', with the objective of creating a 'networked battlespace' in which 'information dominance' has been fully achieved.[48] The American defence industry, in contrast to European firms, has been strongly encouraged to develop C4I (command, control, communications, computers and intelligence). Moreover, the Pentagon is able to draw further strength from advances in commercial and civilian technologies in which the United States is a world leader. This predominance has profound consequences for the future of transatlantic military cooperation.[49]

These consequences are already visible. During the first Gulf War in 1991, French forces encountered severe difficulties with allied interoperability in the area of command and communications. In Bosnia and Kosovo the UK encountered similar problems. When planning Operation Enduring Freedom in Afghanistan in 2001 the United States received many offers of military assistance from European partners but rejected most of them, preferring to avoid the restraints of a wide coalition and the burden of supporting weak allies in the field. Currently, decisions as to whether the US acts unilaterally or multilaterally are still partly political; in ten years' time they will be largely determined by technology. As the result of the 'revolution in military affairs', the United States will find itself unable to interoperate with lesser forces, and NATO will find itself providing various forms of follow-on support, from medical services to military policing. In other words, the information and technology gap will relegate NATO to washing the dishes.[50]

---

[48] The most sophisticated account is offered by B. Berkowitz, *The new face of war: how war will be fought in the 21st century* (New York: Free Press, 2003).

[49] Paul Kennedy, 'The eagle has landed: the new US military position', *Financial Times Weekend*, 1 Feb. 2002; T. Gury and R. Callum, 'The transformation and future prospects of Europe's defence industry', *International Affairs* 78: 4, 2002, p. 765.

[50] David S. Yost, 'The NATO capabilities gap and the European Union', *Survival* 42: 4, Winter 2000–2001, pp. 97–128.

This trend is accentuated by the US emphasis upon information warfare in all its guises. The United States is surging ahead towards its aim of 'networked battlespace', characterized by the extensive use of pilotless aircraft with real-time video and sigint packages. However, it is also dedicated to information warfare in two other respects. The first is information warfare as psychological operations, including flying television broadcast systems whose C–130 aircraft bear the eye-catching logo 'we fire electrons not bullets'.[51] More recently, the United States launched its satellite-based TV station broadcasting exclusively to the Middle East, Al Hurra. Explicitly designed to compete with Al-Jazeera, its programmes are beamed by satellite from a discreet two-storey black building in the suburbs of Springfield, Virginia. The second is 'netwar', defined as electronic attacks by one set of computers upon another. Both these aspects of information warfare are intelligence-related, and Europe has remarkably little capability in either.[52]

Some might argue that in military terms such a transatlantic division of labour could make sense. European states have been proud of their specialist skill-sets right across the field of low-intensity conflict, counterterrorism, peace-keeping and humanitarian aid. All these activities are accompanied by specialist types of intelligence support and intelligence cooperation. Human intelligence, as much as technical systems, is at a premium in these situations. When the British troops arrived in Kosovo, Richard Holbrooke exhorted them to do what they had done successfully in Northern Ireland. More recently, in Afghanistan, the United States has done most of the invading while the Europeans have been bequeathed the task of nation-building. Yet while this arrangement may be prag-matic, such a stark separation of roles will quickly corrode transatlantic solidarity.[53]

Strenuous efforts are therefore being made to deal with the problem of interoperability. At the November 2002 Prague summit, NATO signed up to a new capabilities initiative which emphasized intelligence and related areas including surveillance, target recognition, command, control and communica-tions. Meanwhile the once numerous NATO commands have now been rationalized into Allied Command Operations and Allied Command Trans-formation, the latter being based at Norfolk, Virginia and focused on new capabilities. Countries that place a high premium on integrated operations with the United States have already initiated defence reviews which focus higher levels of spending on information-led warfare. But notwithstanding these efforts, NATO will lack the core capabilities to work comfortably alongside the United States for some time to come. The Prague summit emphasized the creation of a NATO 'rapid reaction force', but this is more likely to become a sort of glorified peacekeeping force.[54]

---

[51] The US has six Commando Solo aircraft flown by the 193rd Special Operations Wing which are generally tasked by the State Department.
[52] Jim Rutenberg, 'Coming soon to Arab TVs: US', *New York Times*, 17 Dec. 2003.
[53] B. de Jong, Wies Platje and R. Steele, *Peacekeeping intelligence: emerging concepts for the future* (Oakton: OSS International Press, 2003).
[54] NATO press release (2002) 127, 'Prague summit declaration', 21 Nov. 2002. Currently the United States provides most of NATO's intelligence through the Battlefield Intelligence Collection and

NATO has other intelligence-related issues to worry about too. In common with the EU, much of its energy is currently focused on enlargement, which brings both problems and benefits. Within NATO, the intelligence and security aspects of enlargement are led by the longstanding NATO Special Committee (AC/46), in which the heads of the civil security services of the NATO member states participate. The leadership rotates annually, and in 2004 the Danes were in the chair.[55] The Special Committee has held elaborate discussions about working with the security services of the countries that qualify as suitable candidates for NATO membership. Much has been learned from the integration of Poland, Hungary and the Czech Republic in 2002. At first sight some of the attendant tasks appear routine and administrative, including issues of personnel screening and cryptographic security.[56] In practice, enforcing these procedures has been problematic. In early September 2003, Slovakia's prime minister, Mikulas Dzurinda, attempted to fire his security chief, Jan Mojzis on the basis of vague and unspecified allegations. However, Mojzis and his National Office of Safety enjoyed strong British and American support as a consequence of having taken a hard line in granting permissions within Slovakia for handling classified NATO information. Indeed, Wayne Ryzchak, the head of the NATO Security Office, visited Bratislava during this episode. Dzurinda was blocked by his own cabinet and only got his way after a second attempt. NATO has also put both Romania and Bulgaria under pressure to 'clean house' of people judged to be linked too closely with Russian intelligence, and also to introduce greater transparency.[57] This has been accompanied by a great deal of quiet bilateral assistance offered by Germany, the Netherlands and the UK in terms of how modern secret services might relate to democratic institutions. Although this work has been discreet, it is likely to have beneficial long-term consequences for the political cultures of countries that were once terrified by their security organs.[58]

Even more intractable are the legacies of economic problems in Eastern Europe. At the end of the Cold War many leading figures in intelligence, often the best and brightest in their own societies, began new careers in politics or

---

Exploitation System (BICES), a near-real-time all-source system that is fed through a gateway located at RAF Molesworth.

[55] The Special Committee, one of NATO's oldest institutions, was set up on 3 Dec. 1952 at the suggestion of Denmark: Politiets Efterretningstjeneste (PET) [Danish Security Intelligence Service], *Samarbejdspartnere*, http://www.pet.dk/Samarbejdspartnere.aspx.

[56] On the wider issues of expansion see T. Edmunds, 'NATO and its new members', *Survival* 45: 3, Autumn 2003, pp. 107–22.

[57] K. Knox, 'Slovakia/Bulgaria: scandals show that building trust between NATO, new members will pose challenges', RFE/RL 1 October 2003, http://www.rferl.org/features/2003/10/01102003153057.asp. Some of the technical collection services of these three countries have close relations with Moscow. See Beata Balogová, 'Dzurinda unforgiving: _imko must leave', *Slovak Spectator* 9: 36, 22–28 Sept. 2003; Kalin Todorov, 'Spy vs. spy', *168 Tchasa*, 3–9 Oct. 2003; Etienne Boisserie, 'Dzurinda en apnée', *Regard sur l'est* 35, 2004, http://www.regard-est.com/Revue/Numero35/Dzurinda.htm.

[58] For a contrary view that suggests that the impact of alliance in the East will be limited to armed forces structures, see Dan Reiter, 'Why NATO enlargement does not spread democracy', *International Security* 25: 4, Spring 2001, pp. 41–67.

business. In some cases this brought them into contact with organized crime. Some countries, such as the Czech Republic, reformed their services successfully, but others, notably the Baltic states, had little idea of how to do this, so that a corrupt version of the former KGB has remained in place. Even where officials are not involved directly in organized crime, salaries are so low that it is difficult to prevent the leakage of information to criminal organizations.[59]

Despite these problems, substantial intelligence dividends await NATO in the East. Former Warsaw Pact countries have excellent capabilities across the whole spectrum of intelligence-related activity.[60] Some of their capabilities have already been deployed to substantial effect, the most widely publicized being the work of Polish special forces in southern Iraq during 2003. Most East European states are experts in electronic warfare and continue to spend to upgrade these capabilities. Poland has only recently acquired a new generation of military communications intelligence systems. NATO efforts are under way to harness this as an integrated NATO electronic warfare capability. The challenge is to standardize procedures and to develop control and communications.[61] NATO's Consultation, Command and Control Agency is currently preoccupied with the problem of integrating data from a wide variety of non-standard systems.[62]

For both NATO and the EU, the challenge is not just a matter of the 'new' European states, but also of widening patterns of cooperation. The NATO Special Committee has also facilitated security gathering among the 46 states that belong to the Euro-Atlantic Partnership Council (EAPC), including countries such as Morocco. In 2002 they established an EAPC/PfP Intelligence Liaison Unit which embraced the Partnership for Peace (PfP). At the same time a treaty was finalized on the protection of classified information exchanged between NATO and the EU. Like NATO, the Council of the European Union has a security committee which pays growing attention to the exchange of classified EU information with third countries and international organizations.[63]

Divergent analytical frameworks

Although it is apparent that transatlantic intelligence problems exist at all levels, they are most visible at the top, where intelligence meets broad issues of strategy. Different alliance members employ widely divergent analytical frameworks to explain current developments. On 9 February 2004, US Defense

---

[59] The most extensive study of such a transformation is M. Los and A. Cybetowitz, *Privatising the police state: the case of Poland* (London: Macmillan, 2000).

[60] Special forces form an important subset of cooperation that lies beyond the scope of this article. Special forces from nine different NATO countries operated alongside US forces in Afghanistan during Operation Enduring Freedom.

[61] 'Polish COMINT capabilities boosted', *International Defense Review*, 1 June 2003.

[62] NATO NC3A Command and Information Systems, http://www.nc3a.nato.int/organization/cisd.html.

[63] NATO, Prague summit texts, 'Partnership Action Plan against Terrorism' updated 22 Jan. 2003, http://www.nato.int/docu/basictxt/b021112e.htm; Annual Report of the Dutch General Intelligence and Security Service (AIVD) 2002, pp. 53–4.

Secretary Donald Rumsfeld addressed this issue directly and offered some retrospective comments on NATO's fragmented response to the invasion of Iraq in 2003. He identified 'the fact that NATO does not have common intelligence' as a key source of its difficulties. Rumsfeld's contention was that states that create common or shared intelligence estimates enjoy a more joined-up view of the world, and are thus more likely to generate convergent policies. He continued:

To the extent we are all working off the same set of facts, or roughly the same set of facts, the people from our respective countries tend to come to roughly the same conclusions, and to the extent we're not working off the same set of facts, we tend not to; and it seems to me that it may very well be that one thing NATO might do would be to do a better job of seeing that the intelligence capabilities of the respective countries are brought together and that the people in NATO and the capitals of NATO countries are kept tuned into those threats and the kinds of capabilities that we as free people face. We're much more likely to get a faster common understanding to the extent we have a reasonably similar perspective with respect to what the facts are.[64]

At one level this could be read as a wistful expression of Rumsfeld's desire that European countries would go along with Washington's view of what the facts are. At another level it contains the interesting proposition that joint intelligence estimates are likely to be significant in encouraging convergent policy among allies.[65] In relation to Iraq in 2003 the facts do not seem to support this assertion. Indeed, one could argue that on the specific issue of Iraqi WMD, almost all western intelligence services, including the German BND, firmly believed that Iraq had some significant capability in this area. This universal belief did not produce a common alliance policy.[66]

Notwithstanding this observation, Rumsfeld's remarks about the relationship between shared strategic estimates and alliance policy raise interesting questions. To what extent are the strategic appreciations generated by NATO countries about the current situation divergent or even contradictory? Superficially, western security agencies and indeed academic commentators share an agreed narrative about the recent past, which has indeed underpinned efforts towards greater cooperation. Some 50 years of political violence by leftist or separatist groups had accustomed security agencies to terrorism as a form of political communication. Purposive political violence was unpleasant, but the scale of risk was relatively modest, certainly by comparison with military

---

[64] 'Rumsfeld urges NATO intelligence co-ordination, Defense Secretary speaks at Munich security conference Feb. 7', US Department of State press transcript of question-and-answer session, 9 Feb. 2004, http://www.iwar.org.uk/news-archive/2004/02–09–3.htm.

[65] I have argued elsewhere that during the first two decades of the Cold War joint UK–US estimates were largely cosmetic and were certainly ignored by policy-makers in Washington: Richard J. Aldrich, 'British intelligence and the Anglo-American "special relationship" during the Cold War', *Review of International Studies* 24: 1, March 1998, pp. 331–51.

[66] The BND apparently even suggested that Iraq might be nuclear-capable by 2004: see D. Mahncke, W. Rees and W. R. Thompson, *Redefining transatlantic security relations: the challenge of change* (Manchester: Manchester University Press, 2004), p. 176.

threats. Moreover, the explicit agenda and local focus of these groups offered some scope for engagement. The aim was to draw such groups away from military strategies towards political rehabilitation. Arguably these efforts met with some success, in both Northern Ireland and the Middle East.[67]

In both North America and in Europe there is a broad acceptance that there has been a 'transformation of terrorism' over the last decade. This is often characterized as a shift from a political terrorism, with tactical or instrumental objectives, to a religious terrorism, whose aims may not be political and whose violence has no obvious upper limit. Although this was closely associated with the exodus of a quarter of a million radicalized *Mujahedin* from Afghanistan, increasing violence was not exclusively Islamic. Tokyo suffered an attack on the subway using sarin gas by the Aum Shin Rikyo cult, which had reportedly identified Washington DC as its next target. There seemed little possibility of political engagement with these groups.[68] As the British home secretary remarked in March 2004, 'We are in a serious business here. These people do not negotiate, they do not have a platform, they do not have a political stance that we can talk to them about, and they do not have fear of prosecution or punishment.'[69]

However, western security agencies do not agree on their broad analysis of the 'drivers' of the new terrorism. Divergent analysis of the current situation is rooted as much in particular intelligence cultures as in discordant political visions. American intelligence agencies have always preferred to focus upon a single homogeneous opponent. For this reason, the American intelligence community found the shift to the post-Cold War era particularly disconcerting and dealt with it spectacularly badly. Innumerable reports on reforming intelligence to meet the challenges of the post-Cold War world piled up, but little of substance changed. The early 1990s were characterized by Fukuyamist emphasis upon economic competition between liberal democratic states and increasing anxiety about economic espionage by 'friendly spies'. The nefarious activities of the Japanese and the French were frequently discussed. By the mid-1990s this preoccupation had been overtaken by improbable but satisfying predictions of a Chinese naval challenge to American hegemony in the Pacific. This in turn has now been replaced by the uncompromising nature of radical Islam.[70]

It is entirely consistent with this paradigm—a search for specific enemies—that the United States has viewed the current upsurge in terrorism as a 'war on America' rooted in particular regimes. Most of the US National Intelligence Estimate material of the last ten years remains classified, but the broad outlook

---

[67] P. Taylor, *Brits: the war against the IRA* (London: Bloomsbury, 2001), pp. 163–79; S. Shpiro, 'The CIA as Middle East peace broker?', *Survival* 45: 2, 2003, pp. 91–112.

[68] B. Hoffman, 'Intelligence and terrorism: emerging threats and new security challenges in the post-Cold War era', *Intelligence and National Security* 11: 2, April 1996, pp. 207–23.

[69] David Blunkett, minutes of evidence given before the House of Commons Defence and Home Affairs Committees, 2 March 2004, Q58.

[70] B. Berkowitz and A. Goodman, *Best truth: intelligence in the information age* (New Haven: Yale University Press, 2000), pp. 29–40, 166–7.

is captured by recent testimony offered by the US National Security Advisor, Condoleezza Rice, on what she called 'the source of the problem'. Rice spoke about the way in which the United States had rejected 'a narrow war' against Al-Qaeda and the Taleban in Afghanistan in favour of 'a broad war against a global menace'. But, ironically, this supposedly 'broader' effort remains, in American eyes, a war against specific regimes. She continued:

The United States and our allies are disrupting terrorist operations, cutting off their funding, and hunting down terrorists one-by-one. Their world is getting smaller. The terrorists have lost a home-base and training camps in Afghanistan. The Governments of Pakistan and Saudi Arabia now pursue them with energy and force … Because we acted in Iraq, Saddam Hussein will never again use weapons of mass destruction against his people or his neighbors. And we have convinced Libya to give up all its WMD-related programs and materials. And as we attack the threat at its sources, we are also addressing its roots.

The United States is not alone in viewing 'the roots of terror' through this prism. Surprisingly, given the political tensions between them, French agencies have followed the Americans in characterizing the drivers of current terrorism in similar terms, but this has not encouraged convergent policy.[71]

By contrast, other West European states have tended to view the upsurge in religious violence as a symptom of wider problems in the international system. In Britain and Germany this phenomenon is often identified by political intelligence analysts as the price of decades of diplomatic failure in the Middle East, sometimes in a post-imperial context. Security agencies tend to locate this failure in the context of 'problems of globalization'. Globalization, they argue, has resulted in cultural provocation and economic dislocation, rendering diverse communities more receptive to the message of messianic terror.[72] Moreover, globalization offered antagonized groups access to new weapons with which to pursue their objectives. Oddly, the networked world of the twenty-first century is well suited to religious movements which are not state-based and which exploit the very transnationalism that developed states have facilitated. A globalizing world is less amenable to state-based security agencies that have depended on boundaries to create choke points through which security threats can be tracked and monitored.[73]

Yet other countries, particularly EU accession states and NATO enlargement states, remain on the periphery of this debate. Although most of the 'new' European partners publicly backed the operations in Afghanistan and

---

[71] National Security Advisor Dr Condoleezza Rice, opening remarks to the National Commission on Terrorist Attacks upon the United States, Hart Senate Office Building, Washington DC, 8 April 2004, http://www.globalsecurity.org/security/library/congress/9–11_commission/040408-rice.htm.

[72] On 7 Nov. 2002 Dr August Hanning, chief of the BND, gave the keynote address at a BND symposium hosted at Pullach entitled 'Globalisierung + Islamismus = Kampf der Kulturen?': see http://www.bundesnachrichtendienst.de/infos/symposien/sym_2002.htm.

[73] This line of argument follows R. Scruton, *The West and the rest: globalization and the terrorist threat* (London: ISI Books, 2003).

Iraq, this had little to do with their interpretation of the structure of terrorism. Terrorism remains quite low on the agenda in Prague and Budapest, beset as the Czech and Hungarian governments are with their own security issues that have little to do with international jihad. While these new member states have been active in providing troops for expeditionary forces, their contributions are primarily symbols of commitment to European institutions.[74]

Conclusion

Intelligence cooperation is the most important weapon in the struggle to contain the 'new' terrorism, but its significance is even greater than that. Across a range of post-Cold War issues, globalization has undermined many of the familiar mechanisms by which states formerly provided their populations with security. Indeed, organized crime, drug-trafficking, money-laundering and immigration have become 'securitized' precisely because of their increasingly transnational character. With the erosion of the familiar national border post, states have turned to more proactive measures to protect their populations, and these efforts are more intelligence-led. In London the recognition of these trends was apparent as early as 1998 in efforts not only to reverse the post-Cold War contraction in the UK intelligence and security services but to expand them. At the operational level, prompt assessment of and response to inform-ation is now at a premium. It is essential that ways are discovered to share precise information rapidly and confidently, without inundating partners with torrents of useless data. Discriminating between patterns of data-sharing will also help us to protect our privacy while reducing the problem of global anonymity. This is important if we are to meet the aspirations of our democratic societies, which do not want to pay an unacceptably high tariff for their continued security.

Michael Herman has sagely remarked that in the field of intelligence, 'inter-national exchanges are a necessity for international society.'[75] However, the prospects for convergent analytical frameworks are less promising. Politicians are remarkably impervious to objective intelligence and the reporting of contrary evidence rarely impedes the path of a determined policy-maker. Donald Rumsfeld's assertion that if we are all working off 'roughly the same set of facts' we will come to 'roughly the same conclusions' is certainly not borne out by history, or indeed by recent events. Transatlantic intelligence cooper-ation has achieved some remarkable things over the years, but it is not about to deliver greater alliance cohesion. Moreover, across an increasingly diverse western alliance, the interface between strategic intelligence analysis and the core executive is changing at different speeds. In some places analysis is still

---

[74] 'New allies back US Iraq policy', *International Herald Tribune*, 6 Feb. 2003.
[75] M. Herman, *Intelligence services in the information age: theory and practice* (London: Frank Cass, 2001), p. 220.

kept at arm's length from the policy process;[76] in others, objective intelligence reporting is likely to sit increasingly awkwardly with presidential styles of governance which prefer subjective policy advice.[77]

[76] The jury is out on the UK system. Although the Joint Intelligence Committee retains some of its time-honoured values, the policy-making machine around it is changing fast, and that presents some new issues. Peter Hennessy has commented on the difficulties that the UK JIC was encountering even before 9/11: 'At the end of 1999 there were signs that Mr Blair was toying with the idea of ending the traditional (and much-prized) distinction between intelligence analysis and policy advice': P. Hennessy, *The prime minister: the office and its holders since 1945* (London: Allen Lane, 2000), p. 502.

[77] The case for radical change is set out admirably in C. A. Medina, 'The coming revolution in intelligence analysis: what to do when traditional methods fail', *Studies in Intelligence* 46: 3, Summer 2002, http://www.cia.gov/csi/studies/vol46no3/article03.html.