JCMS 2006 Volume 44. Number 3. pp. 625–43

Intelligence-Sharing in the European Union: Institutions Are Not Enough*

JAMES I. WALSH
University of North Carolina

Abstract

The European Union (EU) has developed three institutions to facilitate intelligence-sharing between its Member States: the Berne Group, Europol and the European Union Military Staff. These institutions serve the useful function of creating technical mechanisms for the diffusion of intelligence among national authorities. But they do not tackle the problem of mistrust, which is the key barrier to fully effective intelligence-sharing. This article shows that mistrust of the interests of other Member States inhibits intelligence-sharing, that existing institutions fail to overcome this mistrust and suggest changes that could lead to more effective sharing.

Introduction

The collection and analysis of intelligence is increasingly important for the European Union (EU). European governments require timely and accurate intelligence in order to deal effectively with many of the security threats they face today, including terrorism, the failure of state institutions in the developing world and the proliferation of weapons of mass destruction. One important mechanism for obtaining such intelligence is sharing with other countries. Since the 1990s the EU has created or extended three institutions to encourage and facilitate intelligence-sharing between its members: the Berne Group, which brings together the security services of all of the Member States, Europol, which collects, shares and disseminates intelligence on threats such

* My thanks to the editors and anonymous reviewers for their comments and suggestions.

as organized crime and terrorism, and the European Union Military Staff that analyses intelligence on overseas developments.

The objective of these institutions is to facilitate sharing of relevant intelligence by replacing the patchwork of ad hoc and bilateral intelligence-sharing developed by the Member States since the 1970s. These institutions serve the useful functions of creating technical mechanisms for the diffusion of intelligence between national authorities, including organizing regular meetings of ministers and officials, creating common intelligence databases and sharing information on security practices such as counter-terrorism. But these institutions do not tackle the problem of mistrust. Mistrust in the form of divergent policy interests between the partners to an intelligence-sharing arrangement is the key barrier to successful intelligence-sharing.

In what follows, the article first discusses how the development of an integrated European economy that includes the free movement of people, goods and capital, as well as more tentative steps towards the development of a common security and defence policy, has created stronger incentives for the Member States to share intelligence. It then explains how mistrust over the interests and motives of other states inhibits what could be mutually beneficial sharing and how international and European institutions might be designed to overcome this problem. This is followed by a discussion of the degree of trust between the Member States over the issue of intelligence-sharing and a detailed examination of the Berne Group, Europol and the European Union Military Staff. There is strong, if indirect, evidence that mistrust is in fact a barrier to intelligence-sharing in the EU and that none of the institutions can overcome such mistrust. The conclusion briefly lays out two ways these institutions could be reformed to facilitate more effective sharing. The first is to increase their independent powers to supervise and monitor the intelligence collection, analysis and sharing of the Member States. This approach is likely to founder on the strong opposition of national governments. Instead the article advocates a second strategy of encouraging more secure sharing between smaller groups of Member States as a more effective medium-term response.

I. Incentives to Share Intelligence in the European Union

Intelligence is the collection and analysis of open, publicly available and secret information with the goal of reducing policy-makers' uncertainty about a security policy problem.[1] Intelligence takes raw information and analyses it, placing it in the proper context and using it to draw conclusions about attributes of other actors or about the state of the world that are not directly observable

[1] Warner (2002) considers different definitions of intelligence.

(Hilsman, 1952; Herman, 1996, pp. 40, 69–70). Intelligence-sharing occurs when one state – the sender – communicates intelligence in its possession to another state – the receiver.

Two sets of developments have created stronger incentives since the early 1990s for Member States to share intelligence. First, the EU instituted the free movement of people between its Member States, a single market for capital, goods and services and a single currency. This has reduced national controls on cross-border activities and created a demand for sharing of intelligence about terrorism and other criminal activities (Guyomarch, 1997; Hebenton and Thomas, 1995; Peek, 1994; Thuillier, 2000, pp. 138–41). Second, the development of a EU defence and security policy has led the Member States to integrate some aspects of their defence policy planning, including intelligence on overseas developments.

The free circulation of goods, capital and people within the EU poses four significant challenges to Member States' internal security. The first is that it allows greater scope for organized crime groups to increase the scale of their activities overseas without fear of detection at intra-EU borders. The second threat, which in many cases is closely related to the first, is that it eliminates an opportunity to detect illegal trafficking in drugs, people, or items such as counterfeit goods and components of weapons of mass destruction. Third, the introduction of the single currency and the creation of a single financial market make it easier for criminal or terrorist groups to engage in money-laundering or to move overseas funds gained through illicit activities (Occhipinti, 2003, p. 121). The fourth concern relates to terrorism. Free movement makes it easier for terrorists targeting one Member State to seek safe haven in another Member State. It also makes it easier for international terrorist groups from outside Europe to communicate with each other and organize their activities across the Member States (Delpech, 2002).

The second major change with implications for intelligence-sharing has been the development of common foreign and security policies. The key step for intelligence-sharing was the desire to create a European security and defence policy (ESDP). This began in November 1998 at the bilateral summit between British Prime Minster Tony Blair and French President Jacques Chirac in St. Malo. The two leaders issued a joint declaration on European defence which stated that 'the Union must have the capacity for autonomous action, backed up by credible military forces, the means to use them and a readiness to do so, in order to respond to international crises'. The changes to the EU's responsibilities they envisioned were substantial, including the development of 'appropriate structures and a capacity for analysis of situations, sources of intelligence and a capability for relevant strategic planning'.

II. The Role of Trust and Institutions

Governments contemplating sharing intelligence must trust their partners. Trust exists when the interests of a first actor are 'encapsulated' in or congruent with the interests of a second actor (Hardin, 2002; Coleman, 1990, pp. 91–116; Hoffman, 2002). Diverse research traditions in political sociology (Coleman, 1990; Hardin, 2002), social psychology (Hovland *et al.*, 1953), social constructivism (Wendt, 1999, p. 359) and game theory all identify similar interests as a necessary condition for one actor to trust information communicated by another.[2] This insight is also developed by the small number of scholars that have analysed the conditions necessary for intelligence-sharing (Aldrich, 2004; Richelson, 1990; Johnson, 2000, pp. 152–70). When policy-makers in a receiving state believe that their counterparts in a sending state wish to secure the same outcomes, they know that the sender has an incentive to communicate honestly the intelligence in its possession. Even if it believes the sender to have the capability of obtaining accurate and valuable intelligence, the receiver still might discount the value of the sender's communication if it fears the two states do not share similar preferences over the outcome that results from the policy it selects. Conversely, a sending state is more likely to share intelligence with a receiving state if it trusts the latter to treat the intelligence securely and to use it to act in a manner consistent with its interests. Of course, concerns about trust are not the only barrier to intelligence-sharing. Governments also might worry about becoming dependent for intelligence on a state that uses the relationship to extract concessions on other issues, or reject regular sharing with states that have little valuable intelligence to send them in return. But concerns about trust are paramount in the decision to share, since one or both of the partners to a sharing arrangement hopes to rely on intelligence provided by the other that will permit it to make better-informed policy decisions.

Trust is important for both senders and receivers of intelligence. For receivers, trust is crucial because policy-makers are unable to verify independently the accuracy and reliability of shared intelligence. This creates the possibility that the sending state could deliberately alter shared intelligence to influence the receiving state's subsequent policy choices in a direction that serves the interests of the sender but not the receiver. Receivers may be unable to detect such manipulation for two reasons. First, policy-makers in modern states rarely seek access to the individual pieces of information and analytical procedures that comprises intelligence, instead relying heavily on analysts to process such information. They typically lack the time and expertise to analyse raw

[2] Game theory typically does not use the term trust, but works on 'cheap talk' analyses when a receiver will believe information communicated by a sender (see the seminal paper by Crawford and Sobel, 1982). An important application to international politics is Kydd (2000).

information directly and must draw on the expertise of others to place it in the appropriate context. Second, intelligence draws on both open sources of information – those that are publicly available – as well as secret or clandestinely obtained information that the target of analysis wishes to conceal. Intelligence agencies rarely disclose the full details of their sources even to other agencies of the same government. They are particularly reluctant to share full details with other countries out of concern to protect the clandestine 'sources and methods' used to obtain intelligence.

A sender may violate the trust of a receiver in at least three ways. First, a sender may simply lie, that is, alter or fabricate the intelligence it shares with the intent of influencing the receiver's subsequent policy choice. A second and related form of reneging occurs when the sender has accurate intelligence but chooses not to share this with the receiver. The motive is the same; the sender withholds intelligence that might lead the receiver to implement a policy choice that harms the sender. Third, the sender might exaggerate the accuracy of its sources, claming to have quite precise and useful intelligence that it does not in fact possess.

Sending states also need to trust receivers. A sending state must worry that the receiver will use intelligence in a way that does not correspond with its interests. Receivers may violate the trust of a sender in three ways. First, a receiver might deliberately share intelligence with a third party. This constitutes reneging since intelligence-sharing agreements usually prohibit sharing with other states or actors. In such cases the receiver believes that its interests are best served by passing along the intelligence in violation of the agreement, perhaps as a way to influence the third state's foreign policy, but the original sender would find this to be contrary to its interests. Second, the receiver might inadvertently share intelligence in its possession with others. Individuals that have access to its intelligence may be operating under the control of a third state or other outside group and violate their government's policy by sharing this intelligence with their controllers. Sending states therefore try to evaluate carefully the loyalty of individuals and politically influential groups in the receiving state before sharing intelligence. Senders who themselves have received intelligence from another state should be particularly concerned about this sort of reneging, since it might lead the other state to lower its confidence that the intelligence it shares will be treated securely. For example, the fact that Britain depends on intelligence it receives from the United States may make British policy-makers wary about sharing too frequently with European countries if doing so raises questions in Washington about Britain's reliability (Grant, 2000, discusses this case in detail). Finally, concerns about civil and political rights might preclude one state from sharing intelligence with another. Such states might be reluctant to share intelligence in their possession with receiv-

ers who have weaker data protection laws or norms. Such concerns about data protection are particularly important in the EU, whose members have varying commitments to uphold the privacy of personal data. But it is not the only, or even most important, barrier to the sharing of intelligence.

A great deal of research has shown that international institutions and agreements can help states overcome mistrust and engage in mutually beneficial co-operation (Keohane, 1984; Koremenos *et al.*, 2001). Institutions can encourage co-operation even when the degree of trust between the states involved is not very high. They do so through two types of mechanisms. First, institutions can increase the costs of reneging on an agreement. For example, institutions often carefully define what actions constitute compliance and defection and lay out actions that states harmed by reneging can take in retaliation. When effective, these mechanisms increase the cost of defection by clearly and publicly tagging the violating state. This both removes the immediate benefits that the states might hope to secure by reneging and harms its reputation for honest dealing, making it unlikely that other states will sign potentially beneficial agreements with it in the future. Second, institutions can also foster trust by creating specific allowances for states to monitor each other's compliance with agreements. One state cannot effectively and accurately punish another that reneges unless it has accurate information about whether such reneging has actually occurred. Applied to the issue of intelligence-sharing, institutions should encourage freer sharing by allowing receiving states to closely and directly analyse the intelligence they receive from senders. For example, agreements to share might require that the sender convey not only their analysis of intelligence on a particular issue, but also some details about how the underlying raw intelligence was obtained, insights into the reliability of these sources and so on. This allows the receiver to monitor more effectively the degree to which shared intelligence is based on accurate and reliable sources and has not been tainted in the analysis process by the interests of the sending government. Successful sharing agreements might also allow the sender to monitor closely how the receiver uses and disseminates shared intelligence.

A good example of this sort of monitoring is the UK–USA agreement which governs the sharing of signals intelligence between the United States, the UK and a few other countries. This agreement includes safeguards that protect the interests of both senders and receivers. For example, the agreement is believed to include rules about how widely a receiving state can disseminate shared intelligence within its government. It establishes common security procedures and standardized technical terms, code words and training across the participating countries' intelligence services, ensuring that shared intelligence is handled in a consistent manner and is unlikely to be misinterpreted by a receiving state. The agreement also clearly specifies what types of intelligence should

and should not be shared; in general, governments choose not to share intelligence only if it concerns bilateral or commercial issues, deals with sensitive counterintelligence information, or has been obtained through sharing with a third state (Richelson and Ball, 1990; pp. 142–6, 257).

III. Intelligence-sharing in the European Union

Do the Member States of the EU have sufficient trust in each other to share intelligence effectively? How, if at all, do EU institutions facilitate sharing? In what follows, three institutions are first described – the Berne Group, Europol and the European Union Military Staff – that the Member States have developed to support the sharing of intelligence. The article then analyses these institutions' capacity for monitoring compliance with agreements to share intelligence, focusing in particular on their capacity to detect and punish reneging on such agreements and present some indirect indicators of the degree of trust that Member States have in each other in this area. Member States seem to have too little trust in each other to share fully and completely. While these three institutions serve the useful function of maintaining technical facilities for supporting sharing between Member States that do trust each other, they have little capacity to overcome mistrust by detecting and punishing defection on agreements to share.

Sharing Institutions

The Berne Group, or Club of Berne, was formed in the 1970s as a forum for the security services of six EU Member States. It now has 27 members, including all Member States and the chair of the group rotates in tandem with that of the Union. The Berne Club serves as the principal point of contact of the heads of national security services, who meet regularly under its auspices. The Club has established working groups on terrorism and organized crime and in 2001 created the Counterterrorist Group (CTG) in which the Member States, as well as the United States, produce common threat assessments that are shared between the membership and with some Union committees (Council of the European Union, 2004, p. 4; Secretary-General, 2004). The Berne Group does not base its activities on a formal charter and operates outside of the institutions of the EU. There does not appear to be a formal commitment, or even expectation, that participants will share all relevant intelligence in their possession with other members.

The European Police Organization, or Europol, was created by a convention signed by all Member States in 1995 and began operations in 1999. An important predecessor to Europol was the Trevi group, created by the Member

States in the 1970s as a part of European political co-operation. Trevi was an intergovernmental forum with no role for the Commission or European Parliament. The Member States' interior ministries and security services used the Trevi group to co-ordinate national counter-terrorism efforts that had cross-border implications. Trevi established secure communication links between Member States to share intelligence on terrorism and sponsored the exchange of information on training and equipment and investigative methods. Like the Berne Group, Trevi had no formal requirement that states share relevant intelligence; furthermore, it had no permanent secretariat or staff and did not engage in independent analysis of intelligence (Occhipinti, 2003, p. 32; Woodward, 1994).

Europol's priorities are illegal trafficking in drugs, human beings and vehicles; illegal immigration; terrorism; and forgery, money-laundering and cyber crime that cross national borders (a complete list can be found at Occhipinti 2003, p. 192). Its major objective is to improve the sharing of intelligence on these matters between Member States rather than engaging in security, police, or counter-terrorism operations directly. It encourages intelligence-sharing by obtaining and analysing intelligence provided by the Member States, notifying Member States when it has 'information concerning them and of any connections identified between criminal offences', providing 'strategic intelligence' and preparing 'general situation reports', and, since April 2002, establishing ad hoc teams of staff from Europol and interested Member States to collect shared intelligence on specific terrorist groups (quotations from Europol Convention, Articles 3.1 and 3.2). Europol has a staff of about 65 analysts as well as an equal number of staff on secondment from national governments (Müller-Wille, 2004).

Each Member State is represented at Europol headquarters by a European liaison officer (ELO). Member States are required to supply relevant intelligence to Europol through their ELO, either on their own initiative or in response to a request from the organization. ELOs also are responsible for filing national requests for information from Europol. The key mechanism for intelligence-sharing is the European computer system (TECS), which contains two types of intelligence. The first is the Europol information system, which holds information about individuals and groups suspected of having committed, or being likely to commit, a crime falling under Europol's remit. This information is limited to basic identifying characteristics (such as name, date and place of birth, nationality and sex) as well as information about crimes committed or likely to be committed, suspected membership in criminal organizations and relevant convictions (Europol Convention, Article 8). The second type of intelligence is 'work files' generated by Europol staff and ELOs dealing with the

details of specific offences, including contacts of suspects, potential witnesses and others that could provide relevant information.

Intelligence-sharing to support the European security and defence policy is centred on the European Union Military Staff, which supports the Military Committee and the Political and Security Committee. The Military Staff includes an intelligence division of about 30 responsible for early warning, assessment and operational support on external security matters including terrorism. Each Member State supplies at least one person to work on the Military Staff and to maintain secure communication links with their national security agencies. These seconded staff members serve a function analogous to that of the ELOs in Europol. Member States use their representatives to supply intelligence to the Military Staff and to communicate intelligence from the division to relevant national agencies. The division uses intelligence shared by the Member States, in addition to intelligence gathered by EU bodies, to produce assessments for the Military Committee, the High Representative for foreign policy and other EU bodies. Another body concerned with sharing is the situation centre, which collects and analyses intelligence gathered from Member States and others for the High Representative. Some of the situation centre's staff is supplied by the intelligence division; as of 2004 it included one staff member seconded from seven different Member States (Secretary- General, 8 June 2004; Assembly of the West European Union 2002, paras 64–5; Tremlett and Black, 2002).

Trust, Institutions and Sharing

One might agree with the hypothesis that mistrust in the form of divergent interests is the key barrier to intelligence-sharing, but conclude that the actual level of mistrust between EU Member States is quite low. Such a conclusion has quite a bit of face validity. The fact that the Member States have created and ceded a degree of authority to the EU far greater than that possessed by any other international organization might itself be seen as a strong indicator of high levels of mutual trust. Furthermore, the Member States face similar threats to their security. Geographic proximity means that many Member States are directly threatened by security problems at the periphery of the EU in eastern Europe, the Caucuses and the Mediterranean. Many of the Member States have faced or do face serious threats from domestic terrorist groups that operate across borders, as well as from Islamic terror groups. Transnational organized crime also afflicts many of the Member States. If trust is high between the Member States, then intelligence-sharing should occur freely and there should be little need for international institutions that monitor compliance and punish reneging.

The most direct way of determining the degree of trust that exists between Member States would be to investigate their willingness to share operational intelligence. Unfortunately information about the degree of sharing in actual cases is impossible for outsiders and, in many cases, for the Member States themselves to obtain in a reliable manner. Security services are extremely reluctant to divulge such information, even with other agencies of the same national government. Furthermore, there is no guarantee that cases in which information about the degree of sharing that has occurred is available are representative of the universe of relevant cases, as governments may be most likely to release such information only when the sharing has resulted in successful operations. For these reasons the degree of mutual trust in the issue area of intelligence-sharing is assessed through three indirect strategies. First, the rules about sharing in the Berne Group, Europol and ESDP are analysed. Much more information is available about these rules than about the extent of sharing in specific cases. These rules are the product of negotiations between the governments that will share intelligence. The fact that they contain significant limitations on the degree to which participants are required to share intelligence is a good indicator that states demanded these exceptions because they do not trust their potential partners. Second, the degree to which each of these institutions contains monitoring and punishment provisions that would allow states sharing intelligence to overcome mistrust is examined. Finally, the article looks at public comments by policy-makers that express reserve about trust between Member States and indicate that Member States do not fully share intelligence with each other.

None of the institutions has rules that require Member States to share intelligence with each other. Instead, the decision to share is effectively voluntary and left at the discretion of each country. The Member States do not seem to have utilized the Berne Group to engage in significant sharing of operational intelligence. Instead, the Group serves primarily to share ideas about effective tools and policies for countering terrorism and organized crime and for the participating services to understand better the perspectives of their counterparts. There is no requirement or expectation that Member States would share sensitive intelligence that they otherwise prefer to withhold. Gijs de Vries, the EU's counterterrorism co-ordinator, admitted as much, stating that 'it appears that the analysis [of the Counterterrorism Group] does not contribute much to decision-making or to the policy direction of the Union' (de Vries, 2004, p. 11; author's translation). The Club does plan to create a shared database on terrorism and organized crime within the next five years, but this would only 'allow the collation of contextual intelligence on suspects' and 'would not contain sensitive material' (Aldrich, 2004, p. 739).

Europol has detailed restrictions on how its analytical files can be shared and accessed. 'If an analysis is of a general nature and of a strategic type', all Member States may access the report. But if it 'bears on specific cases not concerning all Member States and has a direct operational aim', the only Member States that can access the report are those that provided the initial information leading to the opening of the file, 'those which are directly concerned by that information', and others these Member States invite to participate. Other states may learn about the existence of the analysis file through a computerized index and may request access. But the originators of the intelligence may object, in which case the Europol Convention holds that access shall be agreed by 'consensus', which would seem to give these states a veto over the sharing of Europol's files. In addition, 'the Member State communicating an item of data to Europol shall be the sole judge of the degree of its sensitivity and variations thereof. Any dissemination or operational use of analysis data shall be decided on in consultation with the participants in the analysis. A Member State joining an analysis in progress may not, in particular, disseminate or use the data without the prior agreement of the Member States initially concerned'.[3] Member States may decline to provide intelligence to Europol if doing so involves 'harming essential national security interests', 'jeopardizing the success of a current investigation or the safety of individuals', or 'involving information pertaining to organizations or specific intelligence activities in the field of State security' (quotations from Europol Convention Article 4.5).

Sharing via the intelligence division of the Military Staff has many of the same problems as the Berne Group and Europol. In particular, there is no requirement that Member States share intelligence that might be of value or interest to other Member States or to EU institutions; sharing is explicitly 'voluntary'. As of 2002, there were no arrangements in place for the sharing of very secret intelligence, although one report states that most requests for information are met (quotation from Assembly of the West European Union, 2002, para. 68, 72). The division's practice of collating intelligence provided by national authorities and performing additional analysis circulated under its name means that recipients are not able to identify directly the country that provided the original information. This masking of the identity of the national sources might make Member States worried about security more willing to supply sensitive intelligence to the division (Müller-Wille, 2002, p. 76). Working against full sharing, however, are two points. First, since only seven Member States have foreign intelligence services and these vary widely in their capabilities and coverage of international developments, recipients of shared

[3] Quotations from Europol Convention, Article 10.7; these rules are elaborated in Council Act of 3 November 1998, Adopting Rules Applicable to Europol Analysis Files (1999/C 26/01)

intelligence may be able to make educated guesses about the national source of intelligence transmitted through the division. Second and more importantly, the division receives relatively little 'raw' intelligence from the Member States. Instead, it relies on 'finished' intelligence, which means that sensitive details and sources and methods of collecting intelligence are usually masked from the recipients. Even in those cases where it does obtain raw or operational intelligence, it forwards only summaries to its clients (Oberson, 1998).

The EU also has capabilities to gather and analyse intelligence itself, although these are quite modest in comparison with those of the larger Member States. The EU maintains diplomatic missions throughout the world and has special representatives assigned to specific regions and crises, such as the Balkans, Caucusus, the Great Lakes region of Africa and for the Middle East peace process. These are able to collect openly information from sources such as government officials, publications and so on and through their local contacts may occasionally obtain confidential information. They also may have detailed knowledge of specific issues and can place developments in the proper context for decision-makers. But their diplomatic status means that they are not able to engage in systematic collection or analysis of intelligence. The EU satellite centre in Spain is responsible for processing and interpreting satellite images in support of the EU's common foreign and security policy. But the centre does not actually own or operate its own satellites. Instead, it purchases imagery from commercial satellites and conducts its own analysis. This means that it does not control the tasking of the satellites on which it draws for images, so it cannot guarantee that relevant or timely images will be available. Furthermore, images from commercial satellites are not of the highest resolution and so are useful more as background information rather than operational intelligence (Villesden, 2000). As one investigation reports, 'because of its largely civilian character and the lack of enough appropriately trained staff (military image interpreters) the Torrejón Centre has difficulty in providing the virtually real time imagery necessary to the conduct of military operations during a crisis' (Assembly of the West European Union, 2002, para. 89).

Since the Berne Group, Europol and Military Staff leave it to the discretion of the Member States to determine what, if any, intelligence they will share with their partners, it is not surprising that they all lack strong or effective mechanisms for monitoring or punishing a failure to disseminate relevant intelligence. Voluntary sharing means that there is no direct way for receiving states to ensure that a sharing state has divulged all the relevant intelligence in its possession or to determine that the intelligence has not been modified or distorted to serve the sender's interests. In principle, the assessments or work files produced by staff and liaison officers at the Berne Club, Europol and the Military Staff could allow the detection of deliberately slanted or fabricated

intelligence. Since these assessments draw from intelligence provided by all sharing states, staff and liaisons may be able to detect flaws in intelligence they receive from one national source by comparing it with by intelligence shared by others. But there is no guarantee that they will have sufficient sources of high-quality intelligence from other sources to make such a determination. Such common assessments are not designed as a mechanism for determining if a Member State has withheld relevant intelligence. The Military Staff and Europol do have provisions that provide modest degrees of protection for the interests of sending states. The intelligence division of the Military Staff 'cleans' shared intelligence of information that could identify its source, which gives senders some reassurance that their sources and methods of collection and analysis will not be directly revealed to other states. Europol has detailed requirements about the treatment of shared intelligence pertaining to individuals, which reassures sending states that any concerns they have about privacy rights will be respected by receiving states.

The Member States' security services have managed to share intelligence successfully on numerous occasions. For example, in early 2001 European countries detected a plot by the Al-Qaeda terrorist network to bomb targets in Europe. Intelligence-sharing allowed them to co-ordinate a series of arrests resulting in the apprehension of 18 people as well as weapons and explosives in multiple countries (Swedish Security Service, 2001, p. 31). Despite such successes, however, politicians and officials regularly express concern that sharing is not as open as possible and frequently identify mistrust as the key barrier to greater sharing.

For example, after the terrorist attacks on the United States on 11 September 2001, the European Council meeting of 21 September concluded that 'Member States will share with Europol, systematically and without delay, all useful data regarding terrorism'. Such a statement would not have been necessary if the degree of sharing was felt to be complete (quotation from Council of the European Union, 2001). British Home Secretary David Blunkett repeated this call for more open sharing of intelligence, while acknowledging that Britain would not share its most sensitive intelligence, such as signals intelligence, with other Member States (Black, 2001). Others observed that institutions such as Europol simply could not cope with such difficulties in their present format. Europol Director Jürgen Storbeck complained shortly after the attacks that each Member State was still 'keeping' its information 'to itself' instead of sharing it with others (BBC Monitoring Europe, 2001; Kirk, 2001). The Director of the Belgian Federal Police, Patrick Zanders, argued that an insufficient supply of intelligence from the Member States made it difficult for Europol to respond effectively to requests for information (Convention Européenne, 2002).

Similarly, after the terrorist attacks in Madrid in March 2004 ministers and senior officials stated that greater sharing would help their counter-terrorism efforts, but that mistrust made such sharing unlikely to materialize. French interior minister Nicholas Sarkozy pointed out that creating a stronger EU intelligence capability would be difficult because of the need felt by each Member State to protect its sources. Irish Justice Minister Michael McDowell, then president of the Justice and Home Affairs Council, said that the members had to 'be realistic' in their expectations about greater sharing. Europol's Storbeck again complained that the Member States did not share sufficient intelligence with the agency (European Report, 2004). Belgian Justice Minister Laurette Onkelinx complained that 'there are informal intelligence exchanges at the European level, both bilateral – between two states exchanging intelligence from several countries – and between all the members of what we call the Club of Berne. But this is all informal, there is no obligation, for example, to provide intelligence to a fellow member, there is no obligation to deal with such intelligence at the European level. So the idea is precisely to make such a structure formal and introduce a mandatory element into intelligence exchanges … I believe that Europe must also be built on foundations of mutual confidence, otherwise there will be no sense to it' (BBC Monitoring Europe, 2004). Blunkett criticized other Member States, including Austria and Belgium, for proposing a new EU intelligence agency when many members were not living up to earlier commitments to share intelligence fully. The European Commission complained openly about Member States' 'culture of secrecy' and called for greater trust to prosecute effectively the counter-terrorism campaign (Evans-Pritchard, 2004).

Conclusion

The members of the EU have good reasons to want to engage in intelligence-sharing. Common policies, including the development of a single economy and common foreign policy, mean that the Member States increasingly face similar threats to their internal and external security. It is not surprising, then, that they have developed institutions such as the Club of Berne, Europol and the Military Staff to facilitate the exchange of intelligence. Effective intelligence-sharing requires that participants hold a strong degree of trust in each other. The available evidence indicates that mistrust is a substantial barrier to full sharing in the EU. The Member States have insisted that intelligence-sharing remain voluntary, have declined to create European institutions with the capacity to monitor and punish violations of promises to share and, in their public comments, suggest that the trust between them is too low to allow full sharing. In particular, the design of European institutions for intelligence-shar-

ing are seriously flawed. The focus in the development of these institutions has been on building technical mechanisms – databases, regular meetings and liaison arrangements – that will facilitate sharing between Member States. The expectation behind this approach is that Member States should share a great deal of their intelligence with their partners. But on many occasions the Member States do not perceive it as in their interests to engage in such sharing on a regular basis because of mistrust. But EU institutions simply are not designed to overcome this mistrust.

How might the EU overcome these barriers to intelligence-sharing? Two broad options present themselves. The first would be to strengthen significantly and centralize the EU's intelligence-sharing institutions. A first step in this direction would be to require explicitly the Member States to share relevant intelligence, rather than allow such sharing to remain voluntary. A second step would be to give the institutions the capacity to monitor Member States' compliance with this requirement. At the extreme, this could involve the creation of a EU intelligence agency responsible for directly collecting and analysing intelligence on its own, as some Member States such as Belgium and Austria have suggested. A more modest but still substantial step in this direction would be the creation of a European agency that had legal right, as well as the staff and other resources, to track closely and oversee intelligence developments in the Member States' services. This option, which has been discussed in a preliminary form in recent years, would probably founder on the opposition of many of the Member States. National governments that do not now trust each other enough to share intelligence fully are likely to also mistrust sharing with a new European institution with more intrusive powers than those of the Berne Group, Europol and the Military Staff. Furthermore, efforts to create a powerful new agency would also encounter significant distributional problems. The larger Member States might be reluctant to place their more capable intelligence services under the supervision of a European agency. These Member States might expect to play the role of sender far more often than the role of receiver and would worry that they could carry most of the intelligence collection and analysis burden while smaller Member States stand back and receive their intelligence. Problems such as these greatly hindered the development of an effective system of centrally managing the intelligence agencies of the United States after the Second World War (Zegart, 1999). No doubt such difficulties would be even greater in an attempt to co-ordinate closely the intelligence activities of 25, rather than one, state.

A second option would be to acknowledge the problem of mistrust and to drop the expectation that full sharing between all Member States is a realistic goal in the near future. Instead efforts could focus on encouraging, rather than discouraging, more decentralized sharing between sub-sets of Member States.

These networks would be composed of Member States that share similar interests and trust each other on a particular issue or problem. One step in this direction could involve the creation of more sophisticated networked databases of intelligence. Such databases might be designed to allow a sender to post a description of each piece of intelligence in its possession. This description would have to be specific enough for potential recipients to determine its potential value but would not contain actionable details of the intelligence or any information about the sources or methods through which it was obtained. Other Member States could inspect this description and request the release of the full intelligence report within a short time period. Such a request could trigger mutually advantageous bargaining between the Member States in which each could demand that the other take steps that would conform with the larger political interests of both. A sender worried about inadvertent sharing with third parties, for example, could insist that the intelligence only be shared with certain offices in the receiver's government and require the receiver to track closely dissemination of the report. Over time, successful sharing facilitated by such databases might engender greater trust between sub-sets of Member States that interact regularly and lead to the development of more institutionalized bilateral sharing. Another step might be to encourage policy-makers to meet with subsets of their colleagues from other Member States. For example, the interior ministers of Britain, France, Germany, Spain and Italy already meet regularly to discuss matters of common concern before the full meetings of the Justice and Home Affairs Council (Ferenczi, 2004). Creating more such informal bodies focused on issues of concern to a subset of Member States might allow these countries to understand better the true interests of their partners and indirectly encourage them to share more intelligence. It might also facilitate agreement on new policy measures by all Member States. If one sub-set of Member States acts jointly and successfully, others may choose to follow its lead in order to secure at least some influence over subsequent agreements and to ensure that they receive at least some of the advantages of co-operation (Downs *et al.,* 1998).

Moving in this direction would have many of the disadvantages that creating a more differentiated and 'multispeed' EU has in other issue areas. Intelligence databases with more controls over the dissemination of reports could be cumbersome to manage and create some technical barriers to timely and effective sharing. Membership in different sub-sets of Member States might overlap, creating confusion about exactly who is sharing what with whom. Such a development would continue the current problems that senders face in ensuring that receivers do not share their intelligence with third parties. Or it is possible that membership in the sub-sets might harden over time. This could result in little sharing between Member States in different sub-sets

or lead to conflict between blocs of Member States over issues of common concern. Compared to acting under well-functioning centralized institutions, decentralized co-operation could leave unrealized mutually beneficial gains from exchange of intelligence. But it nonetheless might improve on the current practices, in which Member States already engage in extra-institutional intelligence-sharing or withhold relevant intelligence from European institutions. Since the Member States are already reluctant to cede even modest powers to the EU in this area, decentralized co-operation might be a modest and realistic improvement on the status quo.

Correspondence:
James I. Walsh
Associate Professor
Department of Political Science
University of North Carolina Charlotte
Charlotte NC 28223, USA
Tel: +1 704 687-4535
email: jwalsh@uncc.edu

References

Aldrich, R.J. (2004) 'Transatlantic Intelligence and Security Co-operation'. *International Affairs,* Vol. 80, No. 4, pp. 731–53.

Assembly of the Western European Union (2002) *The New Challenges Facing European Intelligence* (Paris: Assembly of the Western European Union).

BBC Monitoring Europe (2004) 'EU Intelligence-sharing Must Be Mandatory'. 19 March.

BBC Monitoring Europe (2001) 'European Police Chief Says Only Scant Information Being Received from USA'. 15 September.

Black, I. (2001) 'On the Brink of War'. *Guardian,* 21 September, p. 8.

Coleman, J.S. (1990) *Foundations of Social Theory* (Cambridge: Belknap Press of Harvard University Press).

Convention Européenne. Groupe du Travail X. (2002) 'Note de synthèse de la réunion du 25 septembre 2002'. CONV 313/02. 10 October.

Council of the European Union (2001) 'Conclusions and Plan of Action of the Extraordinary European Council Meeting'. 21 September.

Council of the European Union (2004) 'Presidency Conclusions'. Brussels European Council 17–18 June.

Crawford, V.P. and Sobel, J. (1982) 'Strategic Information Transmission'. *Econometrica,* Vol. 50, No. 6, pp. 1431–51.

Delpech, T. (2002) 'Le terrorisme international et l'Europe'. *Cahiers de Chaillot*, No. 56 (Paris: European Union Institute for Security Studies).

Downs, G.W., Rocke, D.M. and Barsoom, P.N. (1998) 'Managing the Evolution of Multilateralism'. *International Organization,* Vol. 52, No. 2, pp. 397–419.
European Report (2004) 'Ministers Revamp Anti-Terrorist Policies'. 20 March.
Evans-Pritchard, A. (2004) 'Time to Cut Waffle and Tackle Terror, Blunkett Tells EU'. *Daily Telegraph*, 20 March, p. 10.
Ferenczi, T. (2004) 'Terrorisme: les cinq grands de l'UE veulent harmoniser les procedures d'expulsion'. *Le Monde*, 19 October.
Grant, C. (2000) *Intimate Relations* (London: Centre for European Reform).
Guyomarch, A. (1997) 'Co-operation in the Fields of Policing and Judicial Affairs'. In Stavridis, S. (ed.) *New Challenges to the European Union* (Aldershot: Dartmouth).
Hardin, R. (2002) *Trust and Trustworthiness* (New York: Russell Sage Foundation).
Hebenton, B. and Thomas, T. (1995) *Policing Europe: Co-operation, Conflict and Control* (London: St Martin's Press).
Herman, M. (1996) *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press).
Hilsman, R. (1952) 'Intelligence and Policy-Making in Foreign Affairs'. *World Politics,* Vol. 5, No. 1, pp. 1–45.
Hoffman, A. (2002) 'A Conceptualization of Trust in International Relations'. *European Journal of International Relations,* Vol. 8, No. 3, pp. 375–401.
Hovland, C., Irving, J. and Kelley, H. (1953) *Persuasion and Communication* (New Haven: Yale University Press).
Johnson, L.K. (2000) *Bombs, Bugs, Drugs and Thugs: Intelligence and America's Quest for Security* (New York: New York University Press).
Keohane, R.O. (1984) *Co-operation Under Anarchy* (Princeton: Princeton University Press).
Kirk, L. (2001) 'Total Control Requires Total Surveillance'. *EU Observer,* 17 September.
Koremenos, B., Lipson, C. and Snidal, D. (eds) (2004) *The Rational Design of International Institutions* (Cambridge: Cambridge University Press).
Kydd, A. (2000) 'Trust, Reassurance and Co-operation'. *International Organization,* Vol. 54, No. 2, pp. 325–57.
Müller-Wille, B. (2002) 'EU Intelligence Co-operation: A Critical Analysis'. *Contemporary Security Policy,* Vol. 23, No. 2, pp. 61–86.
Müller-Wille, B. (2004) 'Building a European Intelligence Community in Response to Terrorism'. *ISIS European Security Review*, Vol. 22, April.
Oberson, F. (1998) 'Intelligence Co-operation in Europe: The WEU Intelligence Section and Situation Centre'. In Politi, A. (ed.) *Towards a European Intelligence Policy,* Chaillot Paper No. 34, December.
Occhipinti, J. (2003) *The Politics of EU Police Co-operation: Towards a European FBI?* (Boulder, CO: Lynne Rienner).

Peek, J. (1994) 'International Police Co-operation within Justified Political and Judicial Frameworks: Five Theses on Trevi'. In Monar, J. and Morgan, R. (eds) *The Third Pillar of the European Union: Co-operation in the Fields of Justice and Home Affairs* (Brussels: European Interuniversity Press).

Richelson, J.T. (1990) 'The Calculus of Intelligence Co-operation'. *International Journal of Intelligence and Counterintelligence,* Vol. 4, No. 3, pp. 307–23.

Richelson, J.T. and Ball, D. (1990) *The Ties That Bind: Intelligence Co-operation Between the UK/USA Countries* (London: Unwin Hyman).

Secretary-General, High Representative for CFSP (2004) 'Summary of Remarks by Javier Solana'. SO159/04, 8 June.

Swedish Security Service (2001) *Annual Report 2001* (Stockholm: Swedish Security Service).

Thuillier, F. (2000) *L'Europe du secret : Mythes et réalité du renseignement politique interne* (Paris: IHESI).

Tremlett, G. and Black, I. (2002) 'EU Plan to Pool Anti-terrorism Intelligence'. *Guardian,* 2 March.

Villadsen, O.R. (2000) 'Prospects for a European Common Intelligence Policy'. *Studies in Intelligence*. Vol. ?, No. ?, pp. nos?.

Vries, G. de (2004) 'Discours pronouncé devant la Commission des Affaires Etrangères de l'Assemblé Nationale'. Paris, 22 June.

Warner, M. (2002) 'Wanted: A Definition of "Intelligence"'. *Studies in Intelligence,* Vol. 46, No. 3, pp. ?.

Wendt, A. (1999) *Social Theory of International Politics* (Cambridge: Cambridge University Press).

Woodward, R. (1994) 'Establishing Europol'. *European Journal on Criminal Policy and Research,* Vol. 1, No. 4, pp. 7–33.

Zegart, A. (1999) *Flawed By Design* (Palo Alto: Stanford University Press).