Occasional Papers

n°50

January 2004

Björn Müller-Wille

For our eyes only?
Shaping an intelligence community within the EU

published by
the European Union
Institute for Security Studies
43 avenue
du Président Wilson
F-75775 Paris cedex 16
phone: + 33 (0) 1 56 89 19 30
fax: + 33 (0) 1 56 89 19 31
e-mail: institute@iss-eu.org
www.iss-eu.org

Institute for Security Studies
Institut d'études de Sécurité
European Union
Union Européenne

*In January 2002 the **Institute for Security Studies (ISS)** became a Paris-based autonomous agency of the European Union. Following an EU Council Joint Action of 20 July 2001, it is now an integral part of the new structures that will support the further development of the CFSP/ESDP. The Institute's core mission is to provide analyses and recommendations that can be of use and relevance to the formulation of EU policies. In carrying out that mission, it also acts as an interface between experts and decision-makers at all levels.*

***Occasional Papers** are essays or reports that the Institute considers should be made available as a contribution to the debate on topical issues relevant to European security. They may be based on work carried out by researchers granted awards by the ISS, on contributions prepared by external experts, and on collective research projects or other activities organised by (or with the support of) the Institute. They reflect the views of their authors, not those of the Institute.*

*Publication of **Occasional Papers** will be announced in the **ISS Newsletter** and they will be available on request in the language - either English or French - used by authors. They will also be accessible via the Institute's Website: **www.iss-eu.org***

The European Union Institute for Security Studies
Paris

Director: Nicole Gnesotto

ISSN 1608-5000
Published by the EU Institute for Security Studies and printed in France by L'Alençonnaise d'Impressions. Graphic design by Claire Mabille (Paris).

Occasional Papers

n°50

January 2004

by Björn Müller-Wille

For our eyes only?
Shaping an intelligence community within the EU

Institute for Security Studies
Institut d'études de Sécurité
European Union
Union Européenne

The author is a post-doctoral researcher at the University of East Anglia. He was a visiting fellow at the EUISS between April and May 2003.

Contents

Summary

Developing international and cross-agency intelligence cooperation has become imperative in today's security environment. If the so-called 'new threats' are to be tackled collectively, it is not only desirable but also necessary to make collective threat assessments.

In contrast to other organisations, the EU applies and has to coordinate a broad range of security policy tools. Therefore, it also needs support from different kinds of intelligence agencies to a larger extent than other organisations. To this end, it has already begun to develop its own structure for the production and exchange of various types of intelligence. At present four EU 'intelligence agencies' can be identified: the fledgling Joint Situation Centre (SITCEN), the Intelligence Division of the European Military Staff (INTDIV), the European Union Satellite Centre (EUSC) and Europol.

This paper argues that the EU does not need any new 'agencies'. Instead it advocates some modification of existing EU 'intelligence agencies' in order to allow them to provide the intelligence support needed for various EU policies. Whereas the present organisation of the INTDIV and the EUSC are regarded as adequate, reforms are proposed for the SITCEN and Europol. The paper emphasises the necessity to strengthen and enlarge the SITCEN, which provides the Union and its member states with external intelligence. Furthermore, Europol should cooperate closer with the agencies of the second pillar (CFSP), and its responsibilities be extended. Apart from adapting existing agencies, the Union should concentrate on facilitating direct cooperation among national agencies in areas that fall under the responsibility of member states. To this end, a European Intelligence Communication Network should be established. One must not be put off by the large technical and political challenges involved in the designing and setting up of such a network, which is necessary because it would allow various European and national intelligence producers to communicate and improve their ability to assess threats. It is also a prerequisite for common assessments, since the Union has only limited intelligence capabilities, in partic-

■ ■ ■

ular collection capabilities, and depends on the support of national agencies. As a result, national and European decision-makers could obtain the support needed for the efficient and coherent national and collective production of security. If the technical standards and the methods, format and content of communications are developed in cooperation with third parties, most notably the United States, candidate countries and NATO, additional points of contact could be established and exchange and cooperation with them enhanced.

Introduction

Often alluded to as the second oldest profession in history, intelligence has become a crucial factor in foreign policy, as well as in collective security and defence.[1] In recent years, intelligence and intelligence cooperation have gained more and more attention.

This development is largely due to changes in the security environment. Intelligence constitutes a core element in the effort to tackle the new kind of terrorism, proliferation, organised crime and even humanitarian disasters. Detecting and assessing the so-called 'new threats' correctly requires increased intelligence cooperation between various intelligence branches as well as between agencies from different countries. Such cooperation is also imperative for the operational implementation of the required multilateral and multi-instrumental responses to the new security challenges.[2]

Given its toolkit, the EU offers a natural framework for intensified intelligence cooperation. In addition, the Union has to develop an intelligence community to match its declared ambitions. Intelligence plays a vital role in the process of developing common security policies and in giving the European Security Strategy substance.[3] To formulate common security policies, Europe needs a common sense of alarm, a common threat perception and thus common threat assessments. Adequate intelligence support will likewise be necessary for the implementation of these European security policies. Current intelligence cooperation must therefore be adapted and restructured in such a way that it can serve common policies that are appropriate to the new security environment.

The question is what role the EU should play and what shape the intelligence community within the EU should have. What kind of intelligence cooperation is needed and reasonable at what level within the EU? Any suggestions for the structure of intelligence cooperation must meet a number of criteria criteria.

- *Deliverability*. Each national and European decision-maker involved in the production of security should receive the intelligence support, i.e. the kind of information, that allows him or her to fulfil his or her responsibilities.
- *Feasibility*. Suggestions should challenge, not drive policy-makers to despair. Therefore, they must build on existing structures for cooperation within the EU and take into account the current division of responsibilities and competencies between the European and the national level.[4]

[1] Phillip Knightley, *The Second Oldest Profession: Spies and Spying in the Twentieth Century* (New York: W.W. Norton, 1988). See also Jeffrey Richelson, *A Century of Spies: Intelligence in the XX Century* (Oxford: Oxford University Press, 1995).

[2] For a closer study on the broader European approach to security see Björn Müller-Wille, *Thinking Security in Europe – is there a European Security and Defence Identity* (Münster: University of Münster, 2003).

[3] 'A secure Europe in a Better World', paper presented by Javier Solana, High Representative for the Common Foreign and Security Policy, European Council, Thessaloniki, 20 June 2003 and approved by the European Council on 12 December 2003.

[4] Thus, although proposing institutional changes, and arguing that institutions matter, the paper acknowledges that the options of change are restrained by (a) the current division of competencies among the Union and various national authorities, and (b) the present structure for intelligence cooperation. This argument borrows from the modified new institutionalist framework for understanding the origins and evolution of security agencies presented by Amy Zegart. In her excellent study, she argues that an agency's evolution can be explained principally by its initial structure, and to a lesser extent by the ongoing interests of relevant political actors and exogenous events. Applied to the subject of this study, the changes in the objective threats against European security interests come in third place, when it comes to initiating and designing institutional changes, i.e. modifications in the structure of intelligence cooperation. See Amy B. Zegart, *Flawed by Design: the evolution of the CIA, JCS, and NSC* (Stanford, Calif: Stanford University Press, 1999).

- *Preservability*. Established bi- or multilateral intelligence relations outside of the EU must not be jeopardised, and it must be possible for third parties (e.g. NATO, the United States and other affected countries) to connect to the intelligence community.
- *Simplicity*. Proposals must support the production of intelligence and thus of security, i.e. facilitate, not complicate, cooperation among participants (agencies from various countries and branches).

The objective of this paper is to elaborate a model that meets these standards. It begins by specifying the term intelligence and what intelligence actors are considered, i.e. what kind of intelligence producers belong to the European intelligence community. This is followed by a short account of the role intelligence plays in the new security environment. Next, general problems encountered in intelligence cooperation are addressed. Thereafter, the specific roles and responsibilities of the EU are determined. This allows for an assessment of how the current intelligence structure within the European Union matches the intelligence support needed for the various European security policy tools. Having done that, the examination comes back to the double challenge of international and cross-agency cooperation. The survey clarifies when a direct exchange between national agencies is preferable, and when the creation of an EU agency makes sense, as well as what regulations for cross-agency cooperation must be formulated at the European level. Section seven, finally, outlines a model for the creation of a European intelligence community, based on the results from the previous sections.

What is intelligence?

Defining intelligence and differentiating it from mere information is not an easy task.[5] In the broadest sense, intelligence can be understood as processed information aimed at assisting a certain receiver's decision-making.[6] What turns information into intelligence often lies in the eye of the beholder. In a security context intelligence assists the receiver in identifying threats, i.e. it helps him or her to become aware of the necessity to take action. In addition, it supports him or her during the planning and execution of field operations or policy actions. One decision-maker may regard certain information as intelligence, because it serves his or her needs, while another considers it to be raw data and mere information. Simplified, the difference can be demonstrated in a matrix with a vertical scale ranging from tactical to strategic decision-making (from operators in the field to policy-makers), and a horizontal one at each level stretching from threat assessment over planning to the actual mission/strike. At lower levels and at the end where strikes are made, real-time single-source 'raw information' can be vital and regarded as the only form of intelligence needed by those leading a mission against a defined target. A move towards the strategic level and to the threat assessment increases the need for basic multi-source assessments or 'finished intelligence' and changes the definition of intelligence. In addition, open-source intelligence (OSINT) usually becomes more important. Policy-makers at this position in the matrix (strategic level – threat assessment) tend to be more occupied with deciding on whether or not to apply any measures, and against or in support of whom, rather than with the question of how and when to intervene.

According to this definition, secrecy and the utilisation of clandestine sources are not considered prerequisites for intelligence. A published assessment based uniquely on open sources can be categorised as intelligence if it is tailored for and helps a specific decision-maker. However, when discussing European intelligence cooperation and the forming of a European intelligence community, publicly available assessments are not of primary interest,[7] but rather the production and exchange of classified information by and among the various national and European intelligence agencies. Thus, for practical reasons, this text operates with an institutional definition of the term intelligence. What makes certain information become intelligence is determined by its origin. Intelligence must pass through one of the institutions that are more or less officially classified as intelligence agencies.

[5] In some cases the differentiation is made even more difficult because the word intelligence is avoided. The UN, for instance, prefers to use the softer term of 'military information' rather than 'intelligence'. See Michael Herman, 'Intelligence After the Cold War: Contribution to international Security?', *Brassey's Defence Yearbook* 1995, pp. 369-83, here, p. 372.

[6] This definition differs somewhat from the more traditional ones. First, this paper only utilises the term intelligence for the produced knowledge – and, ideally, foreknowledge, not for the producing agency or for the utilisation of the knowledge to counteract threats. Second, the term is not restricted to the national level and national security. For various definitions see Thomas Bruneau, 'Controlling Intelligence in New Democracies', in *International Journal of Intelligence and Counterintelligence*, vol. 14, no. 3, 2001, pp. 323-41; Glenn Hastedt (ed.), *Controlling Intelligence* (London: Frank Cass 1991), pp. 6-8; Michael Hermann, *Intelligence Services in the Information Age. Theory and Practice* (London: Frank Cass, 2001), p. 11; Harry Howe Ransom, *The Intelligence Establishment* (Cambridge: Harvard University Press, 1970); Michael Warner, 'Wanted: A Definition of Intelligence', in *Studies in Intelligence*, vol. 46, no. 3, 2002; WEU Assembly Document A/1775, 'The new challenges facing European intelligence – reply to the annual report of the Council', Report submitted on behalf of the Defence Committee by Mr Lemoine, Rapporteur, 4 June 2002.

[7] These assessments can themselves become OSINT in the production of further intelligence. But there is no need to organise the exchange of OSINT at the European level.

Categorising intelligence functions

The production of intelligence is structured differently from country to country.[8] Nevertheless, almost all countries have one or several agencies that to some extent support decision-makers with the following four intelligence functions.

- *Military intelligence* collects and assesses information on actual and potential activities of foreign military forces within and outside its own territory. National agencies producing this kind of intelligence are in general placed under the authority of the ministry of defence.[9]
- *Security intelligence* surveys (domestic) threats targeting the governmental functions defined in the constitution (or equivalent). It is, amongst other things, engaged in surveying counter-espionage, 'left-wing' and 'right-wing' extremist activities and terrorism.[10]
- *Criminal intelligence* engages in the fight against serious and organised crime. It differs from the other functions in the respect that it is linked to criminal investigations, which aim at producing evidence that can result in conviction in a court of law.[11]
- *External or foreign intelligence*, finally, focuses on the development in foreign countries. It supports decision-making on foreign policy in general and produces situation assessments on issues in the fields of security, defence, foreign- and economic policies. As it often makes all-source assessments drawing on military, security and criminal intelligence reports, external intelligence is itself a result of cross-agency cooperation. Nevertheless, in contrast to the functions above, external intelligence supports political rather than operational decision-making. This means that it is less detailed and easier to share.[12]

Categorising intelligence sources

To produce intelligence, one must collect information in one way or another. Authors and professionals often chose to categorise intelligence according to the means by which it has been collected. This distinction can make perfect sense, since one must utilise different means and methods to collect different kinds of information. The most common categories of intelligence sources or collection disciplines are:[13]

- *Human intelligence* (HUMINT), which is derived from human sources, is the oldest form of intelligence collection. It can be obtained through espionage, but the bulk is provided by diplomatic reporting, own field staff, or by the local population.
- *Imagery intelligence* (IMINT) is information from various kinds of images (from photographic, radar, infra-red and other types of imaging devices) that are taken by e.g. persons, aircraft or satellites.
- *Signals intelligence* (SIGINT) intercepts electronic signals of all type. It provides the ability to 'listen' to communications (when needed after encryption), as well as to locate the source of the emission.[14]

[8] This paper does not intend to give an account of the national organisation of intelligence production and the intelligence support given to national authorities in various member states. For a collection of links to different agencies see http://www.fas.org or http://www.geheimdienste.org.

[9] Examples of national agencies in Europe that produce military intelligence are the Defence Intelligence Staff (UK), as well as the Direction Générale de la Sécurité Extérieure and the Direction du Renseignement Militaire (FR).

[10] Examples of national agencies in Europe that produce security intelligence are the Security Service –MI5 (UK), and the Bundesamt für Verfassungsschutz – BfV (GE). For an overview of European security intelligence agencies see François Thuillier, *L'Europe du secret. Mythes et réalité du renseignement politique interne* (Paris : La Documentation française, 2000).

[11] Examples of national agencies in Europe that produce criminal intelligence are the National Criminal Intelligence Service – NCIS and the Metropolitan Police-Scotland Yard (UK), as well as the Bundeskriminalamt (GE).

[12] Examples of national agencies in Europe that produce external intelligence are the Secret Intelligence Service – MI6 (UK) and the Bundesnachrichtendienst (GE).

[13] To those listed one can add Measurement and Signature Intelligence (MASINT). For information about different kinds of intelligence organised according to the method of collection, see for instance US House of Representatives, One Hundred Fourth Congress, Staff Study Permanent Select Committee on Intelligence, *IC21: The Intelligence Community in the 21st Century*, 1997.

[14] The Echelon network, which caused much distress in the mid- and late 1990s, is probably the most prominent example of this sort of intelligence source.

- *Open-source intelligence* (OSINT) is published media and other publicly available information, e.g. internet.

To produce military, security, criminal and external intelligence, agencies can draw on information from any of the intelligence sources, and each collection discipline can serve any of the four different intelligence functions.

Categorising intelligence agencies

Usually, the four different intelligence functions are used to classify intelligence agencies. Most intelligence agencies can easily be categorised as military, security, criminal or external agencies, or as a combination of them, e.g. an agency for military and external intelligence. However, some agencies specialise in a certain collection discipline rather than a function. The collection, processing and evaluation of information from certain sources, e.g. for some signals and imagery intelligence, require expensive technical equipment and highly specialised know-how. Countries cannot afford to duplicate such collection methods within each functional agency. Therefore, this type of high-tech intelligence collection is usually centralised and conducted by a national agency in order to maximise the output.[15] Although such collection agencies, most commonly IMINT or SIGINT agencies, are intended to assist the functional agencies, they also tend to develop their own momentum. Often collection agencies duplicate parts of the functional agencies' analytical capacity. This enables them to develop their ability to steer the collection and interpret the gathered material, at the same time allowing them to give direct support to decision-makers.

[15] The most famous collection agency is probably the US National Security Agency (NSA). A European example is the Government Communications Headquarters (GCHQ) in the United Kingdom.

The role of intelligence in the new security environment

Changing threats

None of the so-called ‘new threats’, such as terrorism, proliferation, organised crime etc., is a new phenomenon as such. The novelty rather lies in the qualitative change of these threats, which results from a combination of several factors. The decline of traditional military threats and a growing vulnerability of modern society have certainly contributed to this trend. The rising number of actors hostile towards and/or able to threaten Western societies and security interests is also important. Most influential, however, is the fact that these antagonists operate on a larger scale than previously, fully using the technologies offered by modern society. The increasing magnitude of threats from terrorism and proliferation illustrates that a larger number of actors are able to pose more serious threats.[16] As a result, the new threats have a more prominent position on the security agenda. This reflects a change in the understanding of security that accentuates three features.

First, the new conception of security no longer focuses on the state level alone. Security actors can be found at the state level, as well as above and below it. The latter can even appear in the form of main antagonists. Ultimately, this new understanding is clarified by the fact that wars are no longer fought between states alone.

Second, the new security conception is multicontextual in the sense that the dividing lines between the genuine military, terrorist, proliferation, criminal and to some extent even humanitarian threats are increasingly blurred.[17]

Third, the new security challenges are transnational with respect to their effect and the geographical place of action. The difference between internal and external threats is disappering.

Changing response

Conceiving and managing different threats as geographically and contextually isolated phenomena is thus often neither adequate nor possible. The new challenges require a comprehensive, cooperative and cohesive approach to security. European and national policy-makers are, therefore, confronted with a double challenge. To a larger extent than ever before, they have to coordinate and interlink the different security policy instruments at their disposal at the same time, as they have to synchronise national and European efforts.

Significance of intelligence and intelligence cooperation

This is where intelligence and intelligence cooperation comes into play. Intelligence has always played a vital role in shaping threat perceptions, i.e. defining threats, and influencing responses.

The importance of intelligence as such has increased, because the new aggressors are more

[16] This is a combination of what Bruce Hoffman calls the ‘amateurisation’ of terrorism and what Harald Müller labelled ‘Megaterrrorism’. See Bruce Hoffman, ‘Intelligence and Terrorism: Emerging Threats and New Security Challenges in the Post-Cold War Era’, in *Intelligence and National Security*, vol. 11, no. 2, 1996, pp. 207-23; Harald Müller, ‘Terrorism, proliferation: a European threat assessment’, *Chaillot Paper* 58 (Paris: EU Institute for Security Studies, 2003).

[17] This is what Peter Andreas and Richard Price neatly describe when they claim that the differentiation between military and criminal threats is gradually being reshaped. Peter Andreas and Richard Price, ‘From War Fighting to Crime Fighting: Transforming the American National Security State’, in *International Studies Review*, no. 3, 2001, pp. 31-52.

difficult to distinguish. This does not only derive from the fact that they act in concealment. Intelligence services have always been engaged in uncovering concealed threats. The new actors are more difficult to identify because of the simple fact that many of the actual assaulters have not displayed any sign of hostility before. The new actors are often unknown and therefore do not fit into the traditional well-known pattern of national allegiances and enmities. In addition, their hostile activities are not always preceded by an escalating conflict between two identifiable parties, as in the case of traditional conflicts between states. Often these threats do not therefore become visible until they materialise, i.e. until the aggressors strike. Terrorists, for instance, may define an adversary and strike without establishing any communication with those targeted. Those engaged in proliferation and organised crime can also be difficult to identify. Not that the main proliferators of weapons of mass destruction (WMD) would be unknown. States that are prepared to export and those having an interest in receiving these weapons and their means of delivery can be identified quite easily. The real difficulties start when non-governmental (criminal) organisations are engaged in the concealed transfer and when the deliveries are no longer made exclusively to other governments and states but also to non-state actors. It is also hard to keep track of the spread of knowledge and expertise, on the one hand, and the export of equipment and ingredients that may be used to produce WMD, (in particular biological and chemical weapons) on the other. Such a development makes it difficult to trace the spread of WMD, as well as to estimate and counteract the threats posed. In short, when you do not know who your adversary is, intelligence becomes critical.

Intelligence also remains vital for the control of compliance with agreements and treaties. Intelligence has proven to be a prerequisite for international disarmament,[18] and becomes increasingly important for the credibility of non-proliferation agreements. The verification capacity is thus indispensable for the formulation of convincing and credible international agreements and policies that limit states' armament.

As intelligence becomes more important, it has to be ameliorated. Surely, one could improve intelligence simply by raising the overall level of effort. However, the current challenges cannot be met merely by 'throwing money at the problem'.[19] The intelligence sector is currently confronted with several challenges.

Developing detectability is the first. Intelligence services must develop new methods and capabilities to ameliorate their ability to detect the new threats so that decision-makers can decide on countermeasures in time.

The second challenge, enhancing cooperation among agencies, is closely linked to the first. Cooperation among agencies is of course a prerequisite to developing methods that allow the intelligence sector to detect the new threats. In addition, sharing intelligence is also often necessary for making accurate and complete assessments of the potential and intentions of traditional as well as new actors, i.e. of the threat they pose. It may be impossible for a single agency to apprehend the full magnitude of internationally operating villains' geographical scope of action, and the field of activities in which they are engaged. A full and comprehensive picture of the threat cannot be obtained if each national agency only takes into account those activities that come within its specific geographical and functional remit. Without sharing intelligence, different security authorities are likely to have different perspectives and will be neither willing nor able to coordinate their efforts to provide security efficiently.

[18] See for instance Herman, 1995, p. 376.

[19] Richard K. Betts, 'Fixing Intelligence', in *Foreign Affairs*, vol. 81, no. 1, 2002, pp. 43-59, here p. 44.

Since the EU formulates and implements its own security policies, the EU also needs its own intelligence support. This poses a third, EU-specific, challenge to the intelligence sector, namely to adapt the production of intelligence to the needs of the EU by developing adequate EU intelligence agencies. This is not possible without intensified intelligence cooperation, this time between the various national and EU agencies.

Finally, cooperation in the field of intelligence is also necessary to deliver adequate and appropriate intelligence support to the various national and European decision-makers, and to allow them to coordinate different instruments and synchronise the countermeasures that various member states and the European Union undertake. Not that intelligence cooperation automatically generates an orchestration of the necessary national and European instruments. Nevertheless, sharing knowledge is a first step towards harmonising views, formulating and implementing common policies, and exploiting potential synergies in the fight against new threats.

Difficulties of cooperation

Sharing classified intelligence is always a delicate matter. Cross-border exchange between national agencies and/or European units is a good indicator of how near the EU countries stand to each other and how close they really are to the declared ambition to produce security collectively. Here, member states reveal to what extent they support (how they interpret) common goals. However, difficulties do not only concern cross-border exchange. Cross-agency cooperation can also be problematic, at both the European and the national level.

4.1 Difficulties of cross-border intelligence cooperation

How can member states' unwillingness to share intelligence with other member states or with European institutions be explained?[20]

The first reason is *distrust*. All intelligence collectors are concerned about the security of their sources and their method of collecting information. If these are uncovered, access to the information will be jeopardised. In addition, they may want to protect the information itself, partly because they are afraid of so-called 'Trojan horses' and partly because they do not want other member states to obtain the information.[21]

The second motive is closely linked to the first. No country wants to jeopardise its *relationship* to other states with which it exchanges intelligence. The United States is the most important counterpart in this context. It seems irrational to share more information within the Union's framework, if this could prompt Washington to reduce, or to stop, the flow of information. This may appear to be the Union's catch-22. As long as there is no credible European alternative to US intelligence collection, the Europeans will not create their own collective capability, fearing that they will get less information. Due to this dependence, independence cannot be achieved. They way out of this dilemma is to make sure that European intelligence cooperation can produce intelligence that is of interest to the United States and thereby also adds value from a US perspective.

The third explanation could be categorised as *financial*. Those states bearing the cost will be unwilling to let other nations become free-riders. Countries will exchange some of the information they have collected with others, not necessarily in a quid pro quo manner limited to the field of intelligence, but in a general exchange.

[20] These arguments were presented earlier in Björn Müller-Wille, 'EU Intelligence Co-operation A critical Analysis', in Contemporary Security Policy, vol. 23, no. 2, August 2002. See also Klaus Becher, Bernard Molard, Frédéric Oberson and Alessandro Politi, 'Towards a European intelligence policy', Chaillot Paper 34 (Paris: Institute for Security Studies of WEU, 1998); Ole R. Villadsen, 'Prospects for a European Common Intelligence Policy', in CIA, Studies in Intelligence, no. 9, Summer 2000; and François Heisbourg (ed.), 'European Defence: making it work', in Chaillot Paper 42 (Paris: Institute for Security Studies of WEU, 2000), in particular chapter five, 'Intimate relations: the issue of intelligence sharing', which draws largely on a contribution of Charles Grant that was published as a CER working paper in 2000 entitled, 'Intimate Relations: Can Britain play a leading role in European defence – and keep its special links to US intelligence?'.

[21] One speaks of a Trojan Horse when a receiver shares the intelligence with third parties that have not obtained the provider's security clearance. One reason for a receiver to pass on the information to others might be that he has friendly relations with a third party, even if the third party is not a member in the same international organisations dealing with security matters. The Scandinavian states could be an example of that or the United Kingdom and the United States. Another reason may be that the receiver swaps information with a third party. This kind of information flow does not always have to contradict the first member state's interests. The decisive factor, however, is that the exchange between the second and third parties cannot be controlled by the one that collected the information in the first place. Moreover, the second state passing the information on may not be aware of the consequences of sharing the information, since it does not know what other intelligence the third party disposes of. What appears as harmless information might turn out to be a decisive piece in a larger puzzle.

Extensive exchange of intelligence reflects trust and tight bonds between the countries involved. The exclusion of some member states, on the other hand, reflects a lack of confidence and solidarity.

The fourth purpose is to ensure one's own country's *influence*. Here, the question is not only whether, or not, information will be passed on, but also when. A large proportion of intelligence is a fresh product, alerting decision-makers and (especially during operations) being used for planning. A lot of classified information will become irrelevant if it is too old, and may become public at a later time anyhow. Intelligence superiority is not only a vital ingredient for operational success; it can also reinforce a country's leadership within a coalition.

On top of this, there are a number of practical difficulties. The most striking one is the linguistic problem. There is no point in forwarding intelligence to others if the receiver cannot understand it. The translation of information into, or direct production in, an accessible language represents a serious additional cost to both national and European services. At the European level, English dominates. Another serious difficulty concerns interoperability, especially of the different information and communication systems. National legislation is a third factor that complicates cooperation. Although member states have agreed on classification regulations for EU documents, difficulties remain at national level. At the time of writing, the national legalisation in some countries had not yet been changed and still hindered the sharing of classified information.

An argument sometimes raised against too much cooperation is founded on the *fear of manipulation*. This issue gained much attention in the aftermath of the 2003 Iraq war.[22] It is quite clear that exchanged intelligence is carefully selected. It is also obvious that states will pick out intelligence and present it in a way that serves their own interests. In some cases, countries might even choose to pass on manipulated or false information in order to misinform and influence others in a certain way. Although this concern is justified, it would be wrong to draw the conclusion that one should refrain from exchange to evade the risk of obtaining false or incomplete intelligence. Any kind of intelligence collection faces the problem of distinguishing between bogus and accurate information. In fact, deception is one of the oldest methods in counter-intelligence. The accuracy can only be verified or falsified if the collection of intelligence is increased, not if it is reduced. This way one is able to compare more intelligence from several sources. By expanding the exchanging, the receivers can ameliorate their ability to evaluate the credibility of different sources. An increased exchange will therefore improve the ability to evade manipulation rather than augment the risk of being directed by others.

4.2 Difficulties of cross-agency intelligence cooperation

In one way or the other, national intelligence agencies of different branches are in contact with each other in each EU country. The established cooperation between branches is, however, often far from optimal. The extent to which national agencies have to cooperate depends on the organisation of the national intelligence community and the nature of the threat being dealt with. Most agencies in Europe were created during the Cold War or even earlier. Over the years the division of responsibilities and the functions of each agency have been clarified and cemented. They have also elaborated their own working methods and developed a proper *esprit de corps*. Some countries have tried to adapt the organisation of the national intelligence community to the new threat environment.[23] The

[22] See for instance House of Commons, Foreign Affairs Committee, *The Decision to go to War in Iraq*, 9th Report, Session 2002-03.

[23] The recent reorganisations in the United States and the Netherlands are examples of such adaptations. It should be noted that the creation of the US Department of Homeland Security has not resulted in a merger of intelligence services. The new Analysis Centre will not duplicate the collection efforts of existing intelligence agencies. Instead, it will draw on reports, assessments, analyses and unevaluated intelligence from the agencies of the Federal Government as well as from law enforcement agencies, state and local government agencies and OSINT. The establishment of a Terrorist Threat Integration Centre (TTIC) which President Bush called for in his State of the Union

adaptation of an agency's competencies or the merger of two or several national services can lessen the reformed agency's need to cooperate with other agencies, and make the exchange of intelligence less urgent. However, it cannot eliminate the need for coordination with other agencies altogether. All European countries are thus still confronted with the challenge of enhancing and facilitating cooperation within the national intelligence community. Nevertheless, cross-agency coordination can be arduous due to responsibility rivalries and 'cultural' differences.

Responsibility rivalries

It is sometimes difficult to make clear separations between the function and areas of responsibility of different types of agencies. In recent years, overlaps have become even more apparent. This development was initiated by the changing security environment that has modified the use of security tools, as well as by ambitions of the agencies. Overlaps can thus be explained by a combination of 'threat pull' and 'agency push'.

To begin with, the activities of rogue actors do not always follow the agencies' division of responsibility and can thus fall within the remit of two intelligence services. Terrorism and other serious crime, for instance, are changing from national to international threats. Furthermore, the 'mix' of intelligence support needed by decision-makers can change as the security environment transforms and the utilisation of security policy tools is modified. The fusion of (new) threats has resulted in a situation where those who decide on and direct countermeasures against organised crime, proliferation, terrorism, etc. need a broader range of intelligence ('threat pull'). As a result, intelligence agencies seek to alter and adapt their collection and production. If, finally, the threat that an agency is to survey is in decline, the intelligence service will try to keep busy by extending its surveillance to new areas ('agency push'). Like other bureaucracies, intelligence agencies have a tendency to maintain their relevance and secure their continued existence both by extending their area of activity and by adjusting their output.

Having agencies with overlapping fields of activities is not necessarily a bad thing, as long as they coordinate their efforts. For external intelligence agencies, overlaps are even imperative, since they also draw on reports from other functional (military, criminal and security) agencies. Overlaps are also normal for SIGINT and IMINT agencies, since it is part of their task to support various functional agencies. Cooperation induced by a 'threat pull' can offer rationalisation advantages and have synergy effects that can be necessary for the production of security. However, this collaboration must be synchronised and organised. If this is not done, overlaps can be counterproductive and rivalries arise. The risk is particularly large when an agency extends its field of action out of self-interest ('agency push').

Reconciling the activities of agencies becomes more important the closer they cooperate with executive authorities. In contrast to external intelligence, which only constitutes one of many inputs to foreign policy decision-makers, the other three types of intelligence are linked more directly to the executive level and

(28 January 2003), in contrast, would merge and analyse all threat information in a single location under the direction of the Director of Central Intelligence (DCI). It seems as if the TTIC will encompass CIA's Counterterrorist Center (CTC) and the FBI's Counterterrorism division, along with elements of other agencies. Encompassing elements from the CIA as well as from the FBI, this merger would do away with the division between internal and external security and bring different branches together. Or as the White House Fact Sheet, 'Strengthening Intelligence to Better Protect America', 28 January 2003, expressed it: 'The Terrorist Threat Integration Center will continue to close the "seam" between analysis of foreign and domestic intelligence on terrorism'. See also Congressional Research Service (CRS) Report for Congress, *Homeland Security: Intelligence Support*, updated 4 March 2003, RS21283.

The Netherlands adapted to the new threat environment by transforming the former security intelligence agency (BVD – Binnelandse Veiligheids Dienst) to the General Intelligence and Security Service (AIVD - Algemene Inlichtingen- en Veiligheidsdienst) and by extending its duties to conducting investigations into other countries. Note the difference between 'binnelandse' (Internal affairs) and 'algemene' (generic). This widens the possibilities of investigating phenomena such as terrorism, illegal migration, etc. See Joy Wijnen Reims, 'Historical Overview: National Security Service (BVD) to General Intelligence and Security Service (AIVD)', *DCAF Conference Paper*, 2002. See also The National Security Service (BVD), *Annual Report* 2001.

have a larger influence on operational direction. It is especially common that security services collect and assess intelligence, while at the same time possessing the power to confront and counteract identified threats directly. Therefore, intelligence overlaps often tend to result in executive overlaps and vice versa. As always, this can cause severe problems. In the worst case, various executive operations may obstruct each other.

'Cultural' differences and problems in cooperating

'Cultural' differences exist among all agencies. The main difference between various agencies' ways of working and 'thinking' can be explained by their relation to the judiciary and the linkage they have to criminal investigations. The cultural difference between criminal and other agencies is therefore also the one that is most difficult to overcome. Criminal investigations are launched when a crime has been committed in order to collect evidence that may result in the conviction of a suspect by a court of law. Running the risk of making an inadmissible simplification, one could say that a criminal investigation focuses on solving a defined crime, while (criminal) intelligence focuses on mapping out the activities of a defined actor. Authorities conducting criminal investigation do, therefore, often work in parallel to intelligence agencies. While criminal intelligence always has a judicial sequel, military intelligence supports military decision-makers and can result in a direct strike against a defined target, usually without aiming at bringing the adversary to court. Security intelligence takes a middle position. It can initiate criminal proceedings, but also result in countermeasures outside of the judiciary, e.g. expulsion of diplomats engaged in espionage. External intelligence, finally, has no direct link to the judiciary, as it makes situation assessments to support foreign policy decisions, rather than supporting operational decisions.

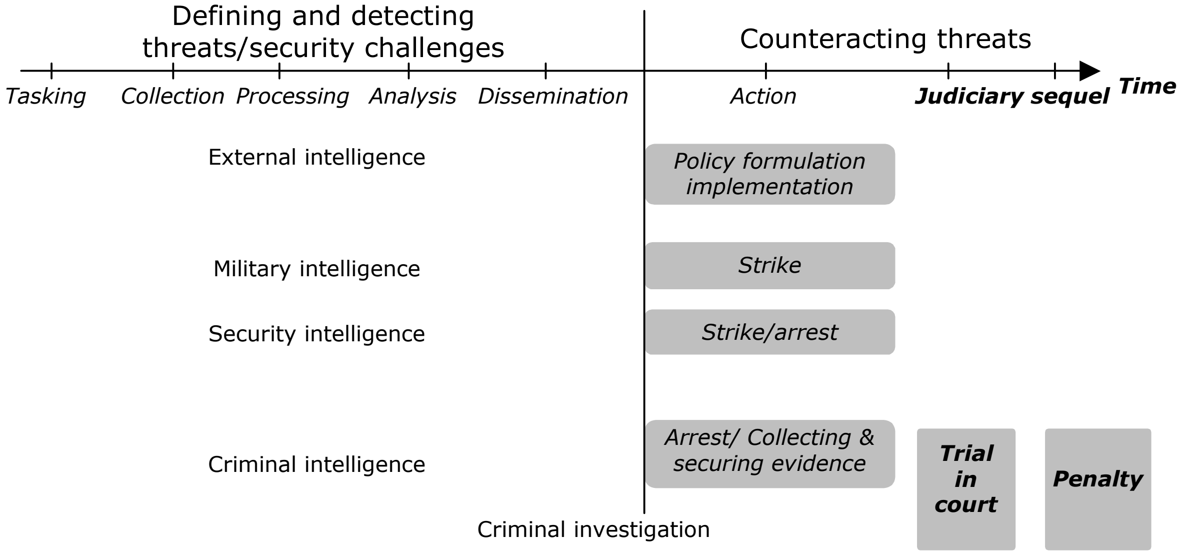

Figure 1: 'Cultural' differences[24]

[24] I thank Michael Jorsback, Special Adviser, Division for Police Issues and Public Order and Safety at the Swedish Ministry of Justice, for clarifying these 'cultural' differences and for the idea of this figure.

The existence or non-existence of a judiciary sequel has a crucial influence on how intelligence is dealt with, in particular the demands made on its accuracy and completeness, and the handling of sources.

Military (and to some extent security) intelligence can support the process by which an enemy is defined and the decision to combat him or her is taken. Such a decision is comparable to a verdict. However, it is not a court that finds someone 'guilty' and defines him or her as an enemy and target. Once this decision is taken, the role of intelligence changes. Military intelligence agencies still have to worry about obtaining the right knowledge at the right time, and providing it to their military decision-makers that determine countermeasures. Operations are preferably launched with precise intelligence, but sometimes decision-makers have to take decisions and launch operations knowing that they have poor intelligence support. The more precise intelligence support is given, the better, but, in a conflict situation, military decision-makers plan and launch assaults against rogue actors on the basis of the available intelligence.

Agencies supporting law enforcement authorities work in a different situation because the supported authority follows another logic. In contrast to military forces, judiciary authorities do not produce security simply by 'neutralising' identified adversaries. They have to seize the 'suspects' and present evidence that can result in a conviction before a court. The requirements of accuracy and completeness are therefore higher for this type of intelligence. Strikes are not simply carried out when the target has been located. If no evidence can be secured, a strike becomes worthless. Usually, attempts are made to keep the collection and production of intelligence in tune with the criminal investigation so that the latter can bring about a conviction before a court of law. Intelligence is, therefore, preferably produced in a way that allows it to be exploited as evidence. It is not simply a matter of what information/evidence is obtained, but also how it was obtained. Whether or not it is gathered in a legal way determines whether it will be accepted by a court.

The handling of sources is the final marked difference. Other intelligence agencies can usually protect their sources and keep informants secret and safe, or in the worst case, can sacrifice them once they have delivered their knowledge and become dispensable. For military (and to some extent security) intelligence, knowledge is crucial, not where it comes from or the fact that it can be verified retroactively. In contrast, a conviction often depends on the testimony of witnesses. Agencies supporting law enforcement authorities are therefore not only interested in knowledge, but also in the persons who have delivered and can confirm it. Protecting sources before, during and after a seizure is thus crucial to the success of an operation. This complicates cooperation between different branches. In the case of military operations, a leak of information can result in reinforced resistance or a relocation of the target. Although this is serious, the operation can be redirected and new plans drawn up to fulfil the mission. A leak of intelligence supporting law enforcement agencies, in contrast, can result in the elimination of evidence and/or potential witnesses. In the worst case, charges may have to be dropped, the operation called off and the targets released. Due to its sensitivity, cooperation in the field of criminal (and to some extent security) intelligence is, therefore, particularly difficult. This intelligence is more sensitive and its secrecy more important for the successful completion of the mission.

Current intelligence support to EU security policy tools

Different EU bodies have different responsibilities and are engaged in the production of security in various fields of activity.[25] This section outlines the kind of intelligence support that is currently needed and provided in each respective field of action. The purpose is to identify shortfalls, i.e. what intelligence needs are not met by the current system, in order to determine where adjustments are necessary. The structure, tasks and responsibilities as they stand at the time of writing are taken as a point of reference. The main reason for this is not simply that the exact outcome of the anticipated Constitution for Europe is difficult to foresee. More important is that the proposals presented by the European Convention and earlier in the Treaty of Nice do not bring about any fundamental changes concerning the intelligence needs at the EU and national level, nor will they automatically do away with the identified shortfalls. The arguments and proposals made on the basis of the current structure will therefore remain valid for some years to come.[26]

The division of responsibilities follows an instrumental and a geographical logic. As for instruments, one can make a schematic differentiation between five fields of action: (1) military, (2) justice (third pillar + rule of law, policing and border guards), (3) civilian and humanitarian (civil protection, demining and humanitarian aid), (4) economic (trade and development aid) and (5) political/diplomatic. In geographical terms, current arrangements make a clear distinction between the internal and external dimensions, and, in each one of these, between the role of nation states and the European Union. The division within the EU structure reveals a strict separation between the internal and external function of the Union as security producer and underlines the nation states' responsibility for all security matters within their national territory. The Union may only take on an operative interventionist role and actively produce security outside EU territory, and maybe along Europe's borders. Within the EU area, the role of the EU in counteracting threats is limited to supporting and assisting national authorities.

To fulfil its tasks in these five fields of action, the EU may need military, security, criminal or external intelligence support. The question to what extent such functional intelligence support is or should be provided by various European units or national agencies is examined below.

Apart from support from functional agencies (military, security, criminal and external), European bodies and decision-makers also obtain assistance from a European collection agency, the European Union Satellite Centre (EUSC) in Torrejon. As the need arises, the EUSC can support the production of intelligence in functional agencies, as well as decision-makers directly. It can thus be active across the five fields of action. The EUSC supports its customers by providing material resulting from the analysis of satellite imagery and collateral data, including aerial imagery.[27] However, the

[25] This section builds on Müller-Wille 2003. For an organisational overview of the EU CFSP and ESDP institutions see International Crisis Group (ICG), *EU crisis Response Capability: Institutions and Processes for Conflict Prevention and Management*, Brussels, 2001, as well as ICG, *EU Crisis Response Capabilities: An update*, Brussels, 2002. See also House of Lords, Select Committee on the European Union, *EU –Effective in a Crisis?*, 7th Report, Session 2002-3.

[26] See also note 32.

[27] See Article 2 of Council Joint Action 2001/555/CFSP of 20 July 2001 on the establishment of a European Satellite Centre.

capabilities of the centre should not be exaggerated. Not that the centre lacks know-how, but, despite its name, it neither owns nor operates any satellites or other collection resources.[28] Its capacity to provide near real-time imagery is also limited. Tasked by the SGHR, the EUSC purchases commercial imagery and obtains some from the French/Spanish/Italian *Helios* I. The EUSC analyses the imagery for, in declining order of priority, the ESDP/CFSP structure within the Council, the Commission, member states and third states or international organisations that have addressed a request to the SGHR.

5.1 Military

With the formulation of Headline Goals and the establishment of the ESDP structure, the member states have clearly expressed their ambition to give the Union a military role. This role is restricted by both geographical and political boundaries. Although no formal maximal distance for the Union's geographical scope has been defined, there is a factual limit to how far away a military ESDP operation can be deployed. A figure often used is 4,000 km from Brussels.[29] It comes from an old WEU illustrative scenario for the most intense type of Peterberg tasks,[30] and was simply determined by restrictions in the available military capabilities for deployment. Although not formally binding, this limitation is still valid for the most intense Petersberg tasks, but less ambitious operations can be launched beyond that distance. In addition, there is a nearer limit. Since the Union's military structure is placed within the framework of the CFSP, it is not foreseen for operations within the territory of the member states. The Petersberg tasks, finally, determine politically agreed restrictions on cooperation.[31] The exact definition of the Petersberg tasks remains somewhat vague. Although they do stretch into peace enforcement (at least in theory, and then only with a UN mandate according to some member states), it seems clear that they do not cover the area of collective defence or preemptive military strikes against suspected adversaries and their acquisition or development of WMD. Nor is overthrowing dictators in the manner recently demonstrated by the United States and others in Afghanistan and Iraq included. Given the current arrangements, member states must pursue such military aims through other organisations or 'coalitions of the willing'. Extending the competency of the Union to such tasks would change the nature of the ESDP and the military intelligence support needed.[32]

The intelligence support to the Union's military structure must, therefore, be geared towards the preparation of potential, and the conduct of concrete, operations within the given geographical and political limits. Hence, the present functioning of the military part of the ESDP does not necessitate the production

[28] See Villadsen 2000.

[29] See Hans-Christian Hagman, 'European Crisis Management and Defence: The search for Capabilities', *Adelphi Paper* 353, 2002, p. 46.

[30] I thank Major-General Graham Messervy-Whiting, former Chief of Staff of the EUMS and currently Deputy Director of the Centre for Studies in Security and Diplomacy at the University of Birmingham, for clarifying this figure to me.

[31] Even if Article 17 (2) of the Treaty on European Union does not explicitly exclude cooperation beyond the Petersberg tasks ('Questions referred to in this Article shall include humanitarian and rescue tasks, peace keeping tasks and tasks of combat forces in crisis management, including peacemaking.'), it can be regarded as a valid restriction, given the intergovernmental structure of the second pillar. This is underlined by the fact that the EUMS 'Terms Of Reference' currently restrict its early warning, situation assessment and strategic planning tasks to the Petersberg tasks.

[32] The adoption of a solidarity clause, as laid down in Article 42 and III-231 of the Draft Treaty establishing a Constitution for Europe, does not necessarily have any impact on the military intelligence support needed. Changes will only come about if the EU itself is to play a coordinating role. It is however possible, and in my opinion likely, that such assistance, including military measures, will be coordinated on a bilateral level, rather than through Brussels. What the introduction of an EU 'Article 5' would imply, as suggested during the Italian presidency of the EU, is not certain either. After an intervention by the non-allied states, the initial proposal of a clear 'Article 5' commitment was bowdlerised with the phrase 'This shall not prejudice the specific character of the security and defence policy of certain Member States'. See IGC 2003, Document CIG 57/1/03, Brussels, 5 December 2003, p. 4; IGC 2003, Document CIG 62/03, Brussels, 5 December 2003, p. 2; IGC 2003, Document CIG 60/03 ADD 1, Brussels, 9 December 2003, p. 33.

and exchange of military intelligence concerning areas in which the Union will not launch military operations, e.g. North Korea and Russia.[33] This is not to say that the design of the current intelligence structure does not allow for such cooperation. It merely means that military intelligence cooperation at the EU level does not have to extend beyond the military ambitions of the ESDP.

The intelligence division (INTDIV) within the EUMS constitutes the focal point for the exchange of military intelligence at the Union level. The thirty national officers in the division compile reports, based on national intelligence, that they disseminate within the ESDP structure. The INTDIV focuses on the military capabilities and on how, and respectively by whom, they are controlled in regions of potential and existing crisis. To some degree, it assesses the intentions of those who possess military power in an area of action. But it does not analyse the interests of actors to the same extent as agencies producing external intelligence do. As a part of the EUMS, the INTDIV supports the strategic planning that starts as soon as a crisis emerges and ends when the EU political authorities approve a military strategic option or a set of military strategic options.[34]

At the time of writing a decision to set up a civilian/military cell in the EUMS had been taken.[35] However, its composition and role are yet to be defined. It seems as if its main task will be to engage when military crisis management missions transform into civilian ones. As it is too early to say anything about its possible involvement with intelligence, the civilian/military cell in the EUMS will not be given further consideration in this paper.

Intelligence support for ongoing operations, in contrast, is not mainly channelled through EU institutions, although the INTDIV opens a line of communication from Brussels to the Operational Headquarters (OPHQ). A detour of national intelligence support via Brussels is not necessary, since the OPHQ, and not one of the Union's own bodies, takes the operational lead. National intelligence is, therefore, fed directly into the line of command to complement deployed forces' own intelligence production.

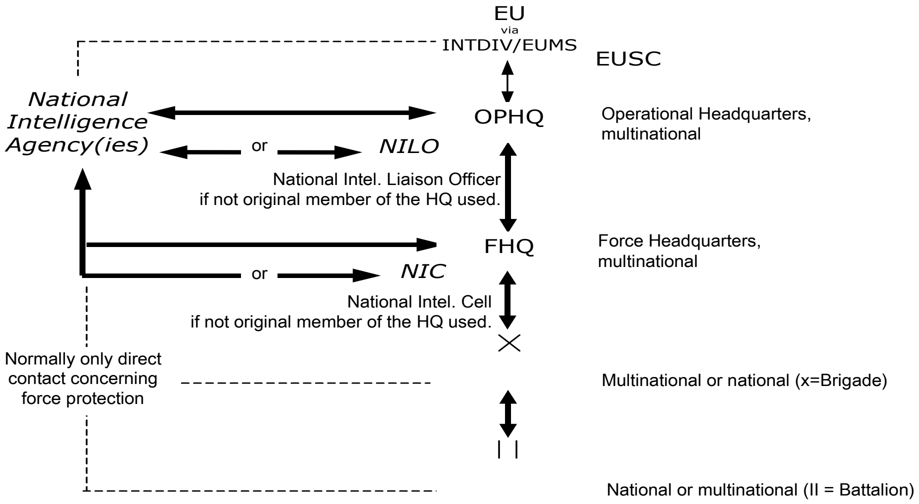
EU
via
INTDIV/EUMS
EUSC
National Intelligence Agency(ies)
OPHQ
Operational Headquarters, multinational
or
NILO
National Intel. Liaison Officer if not original member of the HQ used.
FHQ
Force Headquarters, multinational
or
NIC
National Intel. Cell if not original member of the HQ used.
X
Normally only direct contact concerning force protection
Multinational or national (x=Brigade)
II
National or multinational (II = Battalion)

Figure 2: Intelligence flow for EU military operations

[33] Although this is currently done within the 'East of Europe' concerning Russia, and the 'Rest of the world' section in the case of North Korea.

[34] See footnote 1 of the Annex to Council Decision 2001/80/CFSP of 22 January 2001 on the establishment of the Military Staff of the European Union.

[35] Council of the European Union, *Press Release*, 'European defence: Nato/EU consultation, planning and operations', Brussels, 15 December 2003.

It is quite clear that efficient intelligence support enhances the chances of attaining the objectives of an EU-led military operation and assuring the security of participating troops. The main obstacles to providing such support lie in the limited intelligence collection capabilities of member states, and not in the way current military intelligence cooperation is organised and structured. These capability flaws have been broadly outlined in many different contexts and documents throughout the last years.[36] Despite the possible support from the EUSC to both strategic planning and ongoing operations, imagery intelligence from satellites remains one of the most notable shortfalls. Others are imagery intelligence from unmanned aerial vehicles (UAV) and airborne signals intelligence. HUMINT is also important for all military operations and is sometimes scarce. It is however difficult to speak of a general insufficiency, since access to HUMINT varies a lot from case to case, in particular that provided by the local population.

5.2 Justice, police and border guards

In contrast to the military sphere, the EU is active both within and outside of the EU area in the field of law enforcement. However, the Union does not take on executive functions to the same extent that it does when it leads military missions. Within the treaty area, EU policies are merely intended to simplify cooperation among national law enforcement authorities. Outside EU territory, the Union takes a similar approach. Here the Union primarily seeks to buttress the rule of law by supporting local authorities. It does not pursue a strategy in which European officials replace or override local law enforcement systems.

External EU activities.

In *policing*, the members' goal is to provide up to 5,000 officers for international crisis prevention and management operations.[37] Their main task is, and will be, to provide advice and training in order to develop local authorities. Although executive police functions are not excluded per se, it should be emphasised that international policing is very rare. At the time of writing, international police forces have only taken on this role in East Timor and Kosovo, in both cases under a UN mandate. Given the current arrangements, strikes against criminal or terrorist cells outside the EU by some kind of 'EU police squad teams' will not take place. This will only be feasible if the EU takes over the executive powers of the police as a whole in a 'failed state', or if asked to conduct such an operation by local authorities.[38] As long as that is not the case, EU police missions need little intelligence support, not to say none, in order to fulfil their tasks, namely to advise and train local authorities.

In the field of *rule of law,* member states are to be able to contribute up to 200 experts, including international prosecutors and judges as well as correctional officers who are able to train and monitor staff. Again these are only intended to replace local staff temporarily in exceptional circumstances.[39] As above, these tasks do not require any intelligence support from the EU as long as the Union has not been given a mandate to take on executive police functions, i. e. as long as it is not responsible for producing evidence.

What are needed for both policing and rule of law missions are assessments of the threat against the EU field staff. Thus, the EU field

[36] See for instance the documents and the debates following WEU's Audit of Assets, the European Union's Helsinki Headline Catalogue and NATO's Defence Capabilities Initiative. For a good overview see Hagman 2002.

[37] 1,000 of which are to be deployable within 30 days. See Santa Maria da Feira European Council, *Presidency Conclusion*, Annex I: Presidency report, 19/20 June 2000. See also Göteborg European Council, *Presidency Report*, Annex I to Annex. on Strengthening the Common European Security and Defence Policy, 16 June 2001.

[38] The latter is even more unlikely than the first, since local authorities would most likely turn to a single member state with existing squad teams rather than to the EU that does not dispose of a such.

[39] See Göteborg European Council, *Presidency Report*, Annex III to Annex. See also House of Lords, Select Committee on the European Union, 7th Report, Session 2002-3.

staff do not need any intelligence support to fulfil their task, but the EU needs it when deciding on whether or not to deploy a mission. Recently the SITCEN (see point 5 Diplomacy) assessed risks to the EU police mission in Bosnia-Herzegovina and FYROM.[40]

The envisaged establishment of a European *border guard* is still at the blueprint stage and far from clearly outlined.[41] What intelligence support it will need depends on the responsibilities it is to be given. Some exchange of information between border guards, police stations and consular agents already takes place within the EU through the Schengen Information System (SIS), and the Customs Information System (CIS). Both systems are completely decentralised networks without any central agency. The SIS is best described as a European 'wanted' list, a report system or a search instrument consulted by police, border police, customs and authorities responsible for delivering visas and residence permits.[42] Although the envisaged SIS II seems to be a step from being a mere record of alerts to becoming more of an investigation tool, it does not include the exchange of criminal intelligence. It will not contain any tailored assessments for a specified 'customer', nor be fed by criminal intelligence services.[43] Although all police stations and consular agents have direct access to the network and can enter alerts into it in accordance with their national laws, entries into the SIS do not automatically result in a seizure in another state. Like the Customs Information System, the SIS remains a system for exchange of data upon which national authorities can act, provided they consult the system.[44]

Internal EU activities.

The SIS is complemented by several other arrangements to promote law enforcement within the EU area. Most of them aim at facilitating the exchange of information and cooperation between national law enforcement agencies. Apart from the exchange of liaison magistrates and the establishment of the European Judicial Network (EJN), the EU has also set up a European Anti-Fraud Office (OLAF), Eurojust and Europol. This order corresponds to their relevance in terms of intelligence. Europol is thus the only unit specifically designed to be involved in the exchange of criminal intelligence.

The purpose of the exchange of *liaison magistrates* and the *EJN* is to enable judicial authorities to prepare an effective request for judicial cooperation or to improve judicial cooperation in general.[45] This does not concern the exchange of criminal intelligence.

The administrative investigations conducted by *OLAF* aim at revealing illegal activities affecting the financial interests of the European Communities. For this purpose the office can carry out internal investigations within the Communities' own institutions, bodies and offices, as well as on-the-spot checks of economic

[40] William Shapcott, Head Joint Situation Centre, oral evidence Select Committee on the European Union of the House of Lords, 7th Report, Session 2002-3, p. 17.

[41] See Communication from the Commission to the Council and the European Parliament, 'Towards integrated management of external borders of the Member States of the European Union', COM (2002) 233 final, Brussels, 7 May 2002.

[42] See Article 101 of the Schengen Convention.

[43] 'SIS II takes ominous shape', *Statewatch*, 4 April 2002.

[44] At present the data relates to persons wanted for extradition (Schengen Convention Article 95); aliens who are reported for the purpose of being refused entry (Article 96); persons who have disappeared or who need to be placed provisionally in a place of safety in the interests of their own protection or in order to prevent threats (Article 97); witnesses and persons accused or convicted of offences (Article 98); persons and vehicles for the purpose of discreet surveillance or specific checks (Article 99); and objects sought for the purposes of seizure or of evidence in criminal proceedings (Article 100).

[45] See 96/277/JHA: Joint Action of 22 April 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning a framework for the exchange of liaison magistrates to improve judicial cooperation between the Member States of the European Union. See also Article 4(2) of 98/428/JHA: Joint action of 29 June 1998, adopted by the Council, on the basis of Article K.3 of the Treaty on European Union, on the creation of a European Judicial Network.

operators[46] throughout the EU and even in some third countries.[47] OLAF can be regarded as a collector of data that is forwarded to national authorities in order to initiate and/or support criminal proceedings. In some cases, e.g. if organised crime is suspected to be involved, national authorities may pass this information on to national criminal intelligence agencies. The role of OLAF as a source of criminal intelligence should, however, not be exaggerated. Although it reveals the existence of illegal activities, OLAF does not run any criminal investigation in order to determine who is involved in the crime committed.

Eurojust can be described as a round table of national magistrates. Each national member shall have access to the '. . . information contained in the national criminal records or in any other register of his Member State in the same way as stipulated by his national law in the case of a prosecutor, judge or police officer of equivalent competence'.[48] Moreover, national members shall be empowered to exchange information among themselves or with their member state's competent authorities without prior authorisation.[49] Consequently, Eurojust is the only point where the national criminal records of all member states come together. The members of Eurojust facilitate cooperation among national authorities and may recognise where cooperation is necessary. They discuss concrete cases, exchange information, cooperate directly on a bi- or multilateral level and recommend national authorities to undertake actions. However, that does not make Eurojust a centere for the exchange of criminal intelligence. The reason for this is that the records addressed here usually do not contain criminal intelligence but rather data concerning ongoing or completed criminal investigations.

Europol, finally, plays its proper role in the exchange of criminal and to some extent even security intelligence.[50] It was set up as a clearing house for the exchange of information between member states and given the task of collating and analysing information and intelligence on terrorism, drug trafficking and other serious forms of international crime.[51] Tasked to produce own analysis, Europol is more than an intelligence broker. By compiling and analysing the information from several states, Europol is expected to detect patterns, spot linkages between different criminal activities and draw conclusions that can be decisive in the fight against crime. In this sense, the output from Europol is hoped to represent more than the sum of the input. Nevertheless, one should underline that no responsibilities have been transferred from the national level to Europol, nor has it been given any executive powers of its own. National authorities still hold national agencies responsible for producing and providing the necessary intelligence support, not Europol. It is thus up to each competent national authority to decide on whether or not it will provide Europol with intelligence, follow its advice and make use of the assistance it offers. Therefore, Europol represents but an optional bonus, of which the member states can avail themselves at free will.

[46] Economic operators are such natural or legal persons and other entities on which national law confers legal capacity who have committed the irregularity and to those who are under a duty to take responsibility for the irregularity or to ensure that it is not committed. Article 7 of Council Regulation (EC, Euratom) No 2988/95 of 18 December 1995 on the protection of the European Communities financial interests.

[47] Council Regulation (EC) No 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), Article 3 and 4. Checks in third countries are conducted in accordance with the cooperation agreements in force.

[48] Article 9(4) of 2002/187/JHA: Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime.

[49] Article 13(2) 2002/187/JHA.

[50] On its homepage it presents itself as 'the European Union criminal intelligence agency'. See FAQ on http://www.europol.eu.int.

[51] Article 2 and Annex of the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention).

Note that national agencies supporting law enforcement authorities also exchange security and criminal intelligence outside of the EU structure. As an example, one can note the (supposedly secret but well-known) Club of Berne.[52]

5.3 Civil protection, demining and humanitarian assistance

From an intelligence perspective, operations conducted within the first pillar, i.e. civil protection, demining and humanitarian assistance, are quite alike and, therefore, treated under one heading.[53] While the need for intelligence support for disaster assessments varies, all such operations require similar intelligence support for threat assessments.

Disaster assessments

To begin with, the situation in the affected crisis area must be assessed in order to estimate what kind and amount of assistance is adequate. Although such disaster assessments do not correspond to any of the four intelligence categories presented earlier, technical collection sources utilised by intelligence agencies could support this function. Local HUMINT and real-time IMINT (from military or civilian sources) are of special value for such assessments. Depending on the type of disaster and the resources available to the local government, it can be difficult to get an initial overall picture of the situation. This is particularly problematic for countries outside the EU that have limited assessment capacity and/or when the disaster is accompanied by violent conflict.

Civil protection. Civil protection has been given more attention in recent years. The Union's objective is to facilitate cooperation among the national authorities of member and candidate states. To this end, a monitoring and information centre, and a common emergency communication and information system, have been set up in the Commission's Environment DG.[54] In the light of 11 September one might expect that the purpose is to promote close ties between intelligence analysts and those responsible for assessing vulnerabilities in order to ward of terrorist attacks.[55] This is, however, not the case. The function of this Community mechanism is best described as a clearing house. The purpose is merely to facilitate the mobilisation of intervention teams, experts and other resources in the event of a disaster.

If this occurs in an EU member state, situation and disaster assessments are not produced at the European level, but by competent national authorities, if necessary with the support of temporary EU intervention teams. After some minor adjustments, fellow member states or EU agencies could easily provide the required intelligence support to the responsible national authorities via the affected state's national intelligence agencies.

The difficulties commence if a disaster occurs in a third country without a functioning responsible national authority, e.g. in crisis areas, or in a country that simply does not have contacts with the intelligence services of the countries engaged in the Community mechanism. In such a case, there are no prepared channels through which EU members could compensate for inadequate (or non-existent)

[52] See for instance Hans-Jürgen Lange, *Innere Sicherheit im Politischen System der Bundesrepublik Deutschland* (Opladen: Leske + Budrich Verlag, 1999), p.144.

[53] Although important for crisis management, civil administration is not addressed here, since it is not really in need of any support from intelligence agencies.

[54] Apart from the member states the participation is open to candidates. Article 7 of 2001/792/EC: Council Decision of 23 October 2001 establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions.

[55] This is the leading thought behind the Intelligence section (Directorate for Information Analysis and Infrastructure) established within the newly created US Department of Homeland Security. See Congressional Research Service (CRS) Report for Congress, Homeland Security: Intelligence Support, updated 4 March 2003, RS21283.

intelligence support from the local government's intelligence structure. In the worst case, EU intervention teams would have to take on the responsibility of making disaster assessments and lead the operation. Lacking a prepared channel for intelligence support from EU members, the teams would have to improvise and build up their own support structure.

Demining. The Union's demining activities naturally take place outside of EU territory. It is quite clear that HUMINT and IMINT support is indispensable at the beginning of a demining operation to locate minefields and estimate the magnitude of the mine threat. If mine clearance is conducted by military forces, the intelligence needed to prepare the operation can be obtained from military intelligence channels. Again, limitations only lie in the access to capabilities. However, mine clearance operations are not always conducted by military troops, nor always located in the presence of (international) forces that could provide them with the necessary intelligence. In fact, the EU has only conducted mine clearance operations through its first pillar.[56] Instead of letting EU staff clear the mines, the missions are devised to support the development of local capabilities. Under the direction of the Commission, local authorities are helped with training, equipment and finances. Consequently, the Commission often has to rely on its own personnel contacts (HUMINT) and collect the required information itself, plan its missions and give the necessary support to local authorities once the mine clearance operations are launched. A main deficit is that the European civil bodies involved do not have guaranteed access to (military) IMINT, nor can they task/steer the collection of it.

Humanitarian assistance. The situation regarding humanitarian interventions is somewhat different. The Union's humanitarian aid is channelled through ECHO to those in need outside the EU. For its disaster assessments, the Commission may not be in particularly great need of any technical intelligence support that member states can provide. The Commission usually obtains the necessary information from its own field staff and contacts with other actors in the area.

Threat assessments

When conducted in politically unstable regions outside the EU, disaster assessment must be complemented with assessments of threats against the EU mission on the spot. This is the field of all-source external intelligence. When operating in parallel with international military forces, assessments of threats against EU staff are usually obtained from the military structure. However, the Commission has to make its own assessments of the threats against EU staff when it is not operating in parallel with military units. This has particularly been the case for humanitarian interventions and other aid or assistance projects. Since humanitarian aid decisions are to be taken impartially and solely in accordance with the victims' needs and interests,[57] ECHO's geographical area of operation often does not match those of the Union's other crisis management activities. At present the Commission produces its own threat assessments without direct access to the intelligence apparatus and without being able to task any such agency to produce a situation assessment based on intelligence sources.

5.4 Trade, development

The Union's trade and development policies can certainly be defined as indirect security policies that target root causes. They are, however, not primarily driven by security concerns and do not themselves require any direct support from intelligence agencies. Even if utilised as instruments in support of diplomatic efforts, intelligence support is not necessary for trade and development policies, since that support is given to those deciding on diplomatic issues.

[56] For instance, in Afghanistan, Bosnia and Herzegovina, Croatia, Lebanon and Zimbawe. For information on EU mine clearance actions see: http://eu-mine-actions.jrc.cec.eu.int/demining.asp.

[57] According to 1257/96/EC: Council Regulation of 20 June 1996 concerning humanitarian aid.

5.5 Diplomacy

Diplomacy constitutes one of the main instruments in foreign and security policy. Although external intelligence only constitutes one parameter that influences decision-making in this field, its input is often indispensable.[58] This is not primarily because external intelligence indicates specific policy solutions, but because it outlines the situation in question and is used as a point of reference by which other contributions to the decision-making process can be verified or falsified. External intelligence can provide decision-makers with basic all-source situation assessments (i.e. overviews of actors, interests and developments in a specific area), forecasts/scenarios, threat assessments and in some cases information on the compliance of other actors with security-relevant international agreements.

Within the EU, the Joint Situation Centre (SITCEN), located within the General Secretariat, produces external intelligence. At first the SITCEN was composed of representatives from the INTDIV and the Policy Planning and Early Warning Unit (PPEWU) who were tasked to produce daily reports and press summaries of the current situation in the world. In the last years, however, seven member states have seconded one national intelligence analyst each to the SITCEN.[59] The ambition of the SITCEN has thus increased (although its assessment capability remains very limited with a total of only seven analysts).[60] It has already begun to complement the daily situation reports with general situation assessments of different regions and assessments of threats to EU deployments within the framework of the ESDP.[61]

With a higher aspiration, both the input required by and the information sent to analysts have augmented. Today, the SITCEN obtains intelligence from the EUMS as well as directly from some national intelligence agencies through the seconded analysts. In addition, the SITCEN receives diplomatic reports and other 'non-agency' information. It is on the mailing list of (daily) reports from the Commission's various representations in the field as well as from the EU special representatives. Occasionally, foreign ministries of the member states forward selected reports to the centre. As a result, the SITCEN has become *the* point where different types of national intelligence and 'civil' information are synthesised to all-source assessments and external intelligence.

The SITCEN disseminates its products to the Political and Security Committee (PSC) and to the High representative, the EUMS, EUMC and the PPEWU. Member states and the Commission's DG RELEX can thus obtain the SITCEN products through the PSC. Since the Commission will be fully associated with the work carried out in the CFSP field,[62] DG RELEX has access to the intelligence from both EUMS and the SITCEN. Even if it does not directly pass on intelligence reports to other units within the Commission, DG RELEX can give them advice based on the intelligence obtained.

Unlike other units of the General Secretariat, the SITCEN was not created on the basis of a Council Decision, but on the initiative of the SGHR.[63] Consequently, the tasking and control is also steered by the SGHR. A general direction is given by the 'Watchlist', agreed upon by the SITCEN and DG RELEX on the basis of the 'global overview' which the Council defines

[58] For a closer description of the relation and the difference between diplomacy and intelligence see Michael Herman, 'Diplomacy and Intelligence', Diplomacy & Statecraft, vol. 9, no. 2, July 1998, pp. 1-22, here p. 5.

59 France, Germany, Italy, the Netherlands, Spain, Sweden and the United Kingdom.

[60] Apart from these seconded analysts the SITCEN includes two diplomats from the PPEWU (Policy Unit Front End), three military officers from the EUMS (two from the INTDIV and one from the Operations Division) and a police officer from the police Planning Team. See Shapcott, ibid., p. 16.

61. Shapcott, in Select Committee on the European Union of the House of Lords, 7th Report, Session 2002-3, p. 17.

[62] See Article 27 Treaty on European Union (Treaty of Amsterdam).

[63] This may appear to stand in contrast to Article 207(2) of the Treaty establishing the European Community, which states that 'The Council shall decide on the organisation of the General Secretariat'. However, since the members of the SITCEN are all seconded, formally, it does not necessitate such a decision.

every six months. The latter comprises about 25 to 30 geographical areas of incipient crisis in the world that need to be monitored. Given the limited analysis resources, the SITCEN must set further priorities and decide when to monitor and assess which of the crises on the 'Watchlist'. Three interrelated parameters are decisive for this decision. First, the SGHR tasks the centre to deliver reports in a timely order that matches his or her schedule. Second, the PSC can demand intelligence support. Finally, the SITCEN adapts its production to the development of current events and can produce reports on its own initiative.

As for the shortfalls in the area of external intelligence to diplomatic instruments, one can simply note that the SITCEN is far too small. With the current size, it cannot deliver the external intelligence support needed by EU institutions.

Apart from that, the SITCEN should also be assigned to survey compliance with international agreements, in particular non-proliferation agreements.[64] Many international agreements and treaties directly connected to the field of security, such as the anti-landmine convention, are best controlled with the support of intelligence services.[65] However, the proliferation issue is the most pressing one, and is also regarded as such by the EU. The Union has expressed its commitment to uphold and implement such treaties and agreements, and recently approved an EU strategy addressing the threat of proliferation.[66] To this end, it ought to formulate and implement policies against proliferation of WMD and their means of delivery that go beyond export controls for member states. By signing agreements on voluntary restraints with third parties, the Union could extend and reinforce such treaty regimes. Since the detectability of violations is vital for the credibility of and compliance with such agreements, and thus for their subsistence, the Union must build up its own verification capability. The verification capacity must not only consist of monitoring teams in cases where agreements allow for inspections, but also include an intelligence capacity that surveys compliance. Since non-proliferation falls within the remit of the CFSP, this intelligence function should be assigned to the SITCEN, which has already begun to engage in proliferation matters, for instance by assessing the threat posed by the acquisition of WMD by terrorists.

5.6 Implications for the model of a European intelligence community

Taking the tasks of different EU units as a point of reference, one can note that the main shortcomings concerning intelligence support are to be found in four areas.

- *Collection capabilities*. Capability gaps in the field of technical intelligence collection and for the deployment of these assets constitute a serious shortfall. This restricts the ability to supply the required intelligence support in all fields of EU actions.
- *Civil protection and humanitarian action*. This concerns initial intelligence support, particularly IMINT, to assess the extent of the damage caused by a disaster and assessments of man-made threats to EU staff in the field. The Commission makes the latter alone, without support from intelligence agencies. Instead of being a main consumer of intelli-

[64] In particular the Australia Group (linked with the Chemical Weapons Convention and the Biological and Toxin Weapons Convention), the Zangger Committee and the Nuclear Suppliers Group (linked with the ultimate objectives of the Non-Proliferation Treaty), the Missile Technology Control Regime and the Wassenaar Arrangement.

[65] Convention on the Prohibition of the Use, Stockpiling, Production, and Transfer of Anti-Personnel Mines and on their Destruction.

[66] 'EU Strategy against Proliferation of Weapons of Mass Destruction', adopted by the European Council, 12 December 2003. For more information on the topic in general, see Stephen Pullinger and Gerard Quille, 'The European Union: Tackling the threat from Weapons of Mass Destruction', in ISIS Europe and Saferworld, *Discussion and Policy Papers* (2003).

gence, the Commission is thus primarily a collector.

- *External intelligence*. Since the EU needs external intelligence support for most of its policies, the size of the fledgling SITCEN remains one of the main bottlenecks.
- *Verification capability*. The EU lacks the capability to verify compliance with international agreements that restrain armament, and thus a main component for the implementation of common policies in this field, e.g. a non-proliferation policy.

As for intelligence needs, one should emphasise that member states retain full responsibility for their national security. At present, the EU does not have any executive responsibilities to counteract any of the new threats, be it within or outside the EU area. Therefore, national authorities depend on cross-agency intelligence support to a much larger degree than European bodies. Of course, the Union does need intelligence support for the actions it undertakes. But it is quite clear that the SITCEN is the only EU 'agency' that by nature and task requires access to intelligence from various branches to produce accurate external intelligence. Europol is naturally also dependent on access to criminal and security intelligence to fulfil its task. But in contrast to the SITCEN, there is no EU function that requires, let alone depends on, intelligence support from Europol. The 'customers' of Europol are the national law enforcement agencies, not any EU units.

Finally, clarification might be needed concerning the early warning function of intelligence. One should bear in mind that a situation, which may need a response within the remit of EU actions, will be evident, if not always to the public then at least to practitioners in the field of security, before any Union body delivers a report (at least in current circumstances and in the foreseeable future, as long as the CFSP is intergovernmental). To fulfil its task, the EU does not, therefore, have to identify new problems, risks or threats that nobody else has seen.[67] Given the current arrangements, where national authorities carry the primary responsibility for national security, the early warning function remains at the national, not the European level. Consequently, the responsibilities for detecting and directly warding off threats, irrespective of whether they are foreseeable and preceded by an escalation or not (e.g. envisaged terrorist attacks, proliferation or other crimes), lie with national, not European, agencies and authorities.

[67] This is also valid for the PPEWU, which works on a timeframe of 2-4 months. Its so-called 'early warning' function is geared towards answering how the EU can respond to a certain situation at short notice, rather than to determine what threats may arise within the coming months.

Organising and regulating international cooperation

6.1 Vertical assistance or horizontal coordination?

One of the main questions when shaping a European intelligence community is whether new intelligence agencies are needed at the European level, or whether cooperation should take place between national agencies. There are two basic models for cross-border cooperation. One can either build a system of vertical assistance or seek ways to improve horizontal coordination.[68] Vertical assistance implies the creation of a European body that may produce its own assessments and through which the intelligence from national agencies is channelled. Horizontal coordination, in contrast, is constructed as a network by which national agencies can make direct bi- or multilateral contact and exchange intelligence with each other. Horizontal coordination does thus not include a European 'head'. As shown in the previous section, the EU structure currently accommodates both forms of cooperation.[69]

What model is adequate, and when? The simplest way to answer this is by asking whether or not the creation of a centralised European body adds value. A central European 'head' is recommendable if:

- it produces something that can, is or will not be produced at the national level;
- the responsibility for a certain form of intelligence product is transferred to the European level, i.e. if the European unit can relieve national authorities.

Unless one of these conditions is met, the value added by vertical assistance will be meagre. National agencies will not be particularly keen on feeding intelligence to an EU agency that does not fulfil at least one of these two criteria. That in return will result in an even more modest value added by the EU agency concerned. In this case, one may as well content oneself with horizontal intelligence cooperation.

In order to draw up suggestions as to how a European intelligence Community should be organised, one must examine existing intelligence cooperation within the EU. Should we opt for more vertical or more horizontal intelligence cooperation? To determine this, one must ask if the current EU agencies add value, and why (or why not).

6.2 Does vertical assistance work in the EU?

EUSC. Although the EUSC does not have an exclusive capability, it produces intelligence that most member states cannot produce at the national level. Based on this fact alone, one can conclude that the centre adds value and that the model of vertical assistance is adequate. This is not to say that the centre can satisfy the Union's and the member states' IMINT requirements. However, this does not depend on the chosen organisation. There are two other reasons for this. The first problem lies with the limitations of the product in terms of volume and quality, which depends on the input to the centre, rather than on its ability to processes incoming imagery. The second problem is the customers' limited habit, and therefore their ability to

[68] See Müller-Wille 2003, pp. 144-56.

[69] With its double-hatted magistrates, Eurojust could even be seen as as a mixture of the two.

utilise satellite imagery, incorporate it in their analysis and benefit from it.

INTDIV of the EUMS. The INTDIV adds value not by producing something that national agencies would not be capable of producing but by providing intelligence support that cannot for political reasons be provided by a single national agency. Like the entire EUMS, the INTDIV does not really have a unique capability that most member states lack. Almost all member states possess a military structure for strategic planning and operating their national forces. All of these national headquarters receive support from their own national military intelligence agencies. But since EUMS serves the ESDP structure and not national defence, a national headquarters could not replace it. Such a solution would be unacceptable and counterproductive and would conflict with the multinational nature of the mission that is to be supported. This is why a national intelligence service cannot substitute for the INTDIV. Thus, the value added by the EUMS and the INTDIV does not primarily consist of the intelligence output. Rather, vertical assistance as such represents added value, since it is a perquisite for conducting European Petersberg missions.

SITCEN. It may be a bit early to from an opinion on the practical value added by the SITCEN. Given that it was created by the SGHR and not by a Council decision, it is quite obvious that the centre was meant to give intelligence support to the SGHR. By serving this existing demand it already adds value. Since the Union's external policy is global in scope, the SGHR needs intelligence support with full international coverage on a timescale that is adapted to his or her agenda. This cannot be provided by national agencies. Hardly any national agency surveys all parts of the world, and those that do cover the areas concerned are primarily steered by the programmes of national decision-makers. Provided the SITCEN can draw on intelligence from all member states as the need arises, it will gain access to intelligence with nearly complete coverage and be able to adapt its product to the needs of the SGHR and other customers. The reports from the SITCEN are not prepared exclusively for the SGHR. The SITCEN provides the same intelligence reports to the decision-makers throughout the ESDP structure and thus to the Commission as well as to the member states. This contributes to the harmonisation of their knowledge and may facilitate and influence the formulation of common policies within the second pillar.

Member states usually prefer to conduct their external policy with the support of other states. Since the EU offers a framework for the formulation of a common policy, member states have some interest in making sure that the centre's reports correspond with the information upon which their national position is based. Therefore, they are likely to forward intelligence that supports their interests to the centre. Admittedly, the SITCEN runs the risk of being fed with disinformation. However, such attempts at manipulation will most likely prompt states with diverging opinions to forward their intelligence reports. Provided member states consider the content of SITCEN product important, the centre will thus obtain the necessary information to produce well-balanced and critical reports.

Europol. Due to a conceptual deficit, the value added by Europol is limited. The imperfection does not reflect any inability on the part of its officers, nor is it a result of a lack of resources. It is a problem of structure. In contrast to the EUSC, INTDIV and SITCEN, the providers of intelligence to Europol are identical with the main customers – the national agencies. The incoming intelligence is not processed in Europol and disseminated to another group of decision-makers, but sent right back to the sender. This, in combination with the fact that no responsibilities have been transferred from the national level to Europol, leads to a duplication that sets the limit. Europol can neither relieve national agencies nor produce anything that national agencies do not try to produce themselves. National agencies can never explain failures by referring to a malfunctioning Europol. Since national agencies carry full responsibility for producing the intelligence support required for national security, they cannot be dependent on Europol. Hence, to make sure that they can deliver, national agencies must maintain a complete national product. Simply put, whatever Europol does has to be produced at the national level as well. The incentive for national agencies to feed Europol with intelligence is thus limited. As national agencies cannot pass the buck to Europol, they have preferred to draw on established multi- and/or bilateral contacts and networks, rather than to reinforce the sharing of intelligence through Europol. This prevents Europol from exhausting its full potential. The only way it might add value would be by bringing together expertise and making better analysis, based on intelligence received from a larger number of national agencies, than any single national agency can. But without the necessary input from national agencies, Europol can rarely make a better assessment than its national counterparts. Therefore it can neither take on the role of an intelligence agency nor act as a clearing house in a satisfactory manner.

This is not to say that European law enforcement and criminal intelligence agencies do not need to cooperate. On the contrary, the result of non-cooperation between member states can result in a situation where an internationally operating criminal or a member of a criminal organisation can be arrested and prosecuted for a minor crime in one country. This can disturb, hinder and even block a criminal investigation for more serious crimes in another country, which then has to begin again. Such exchange of information and intelligence can take place through Europol but might also take place on a bilateral level or in the joint investigation teams. Thus, vertical assistance is not a prerequisite for such intelligence sharing.

To conclude, the current mode of cooperation shows that the model of vertical intelligence assistance risks being inefficient unless the European 'head' has a European executive function.[70] The type of intelligence support currently needed by EU institutions, as outlined in section 5, could be delivered by the existing EU 'agencies' if these were modified. As for the intelligence support to policies which fall within the responsibility of member states, the exchange and production of intelligence need not take place within a European 'head'. As the example of Europol shows, horizontal cooperation is quite sufficient, not to say the better option in these cases. The EU thus does not need any new agencies: it just needs to develop and adapt the existing ones.

6.3 What cross-agency exchange can be and needs to be regulated by the EU?

Cross-agency exchange of intelligence is a prerequisite for the coordination of activities of various executive agencies and for their efficient operation. Regulating this at the Union level would not only exceed the competencies of the EU, as national agencies are subject to national law and each state enacts its own rules concerning its agency's exchange of intelligence. Finding a standardised solution that is applicable to and adequate for each individual national intelligence community would also be impossible.

Concerning cross-agency exchange, the Union merely needs to regulate the exchange of intelligence where its own 'agencies' are involved. Whilst relations exist between all three ESDP 'agencies' (INTDIV, EUSC and SITCEN), it is remarkable that there is no linkage between

[70] Here one can draw a parallel with NATO in which the bilateral exchange of intelligence still prevails. Michael Herman (1995, p. 374) speaks of 'the unofficial system of national cells working "behind green baize doors" to give private briefings'. That the Alliance never developed a proficient central intelligence 'head' can easily be explained. NATO offered but an alternative to national operations without limiting national autonomy or relieving the member states of any responsibility, and without any independent (let alone exclusive) executive responsibilities.

them and Europol, which is located within the third pillar. The exchange of criminal and security intelligence that does take place within the EU is thus completely isolated from the other branches. On the one hand this is understandable, since Europol focuses on security within EU territory, while the ESDP structure operates outside it. As the EU has no executive law enforcement functions outside the treaty area, one might also argue that the second pillar does not need any law enforcement intelligence support, and that the intelligence produced and held by the ESDP agencies cannot add value to Europol activities.

However, when considering that the 'new' threats do not stop at the Union's external borders, this division appears somewhat artificial. It may even raise the suspicion that it is counterproductive. This does not mean that the ESDP structure should redirect its focus and be utilised within the EU. Rather, the geographical competency of Europol should be extended. Furthermore, all EU agencies should be interconnected in one way or another and all agencies in Europe engaged in giving the necessary intelligence support to EU security policy tools. This includes national agencies, at least when member states choose to act through the Union. Moreover, they should all be in contact with the potential customers and/or executive bodies that function as collectors and can feed the EU intelligence community with information that is itself utilised in the production of intelligence.

A model for a European intelligence community

The following proposals take the present (and in part envisaged) division of executive responsibilities and the current intelligence needs for EU security policy tools as a starting point. By so doing, the study might present an argument applicable in practice without depending on any unlikely reallocation of executive responsibilities between national and European authorities. Therefore, this section begins by suggesting modifications concerning the tasks of some EU 'agencies'.

The second part of the section addresses the question of how the agencies of the EU, member states and third parties should be linked. It is imperative to find solutions that facilitate intelligence exchange between agencies, without impeding established bi- or multilateral intelligence exchange. Thus, the structure of a European intelligence network will be outlined, and regulations concerning the intelligence exchange commented.

7.1 Developing EU agencies

It is quite clear that the inadequate capabilities for technical intelligence collection set limits on the ability of EU agencies to provide the necessary intelligence support to the EU structure. This is the main reason for intelligence shortcomings in the ESDP area, as well as for the inability to make disaster assessments. Developing suggestions as to how the EU could extend the technical capabilities of member states does, however, go beyond the scope of this study, which focuses on the institutional structure of a European intelligence community.[71] The weaknesses of the EUSC and the INTDIV are directly linked to these capability shortfalls, and not to their organisation. Therefore, these two agencies do not need to be radically restructured, and are not central to the proposals presented below.

The other shortfalls identified in this study, however, could be significantly reduced through a reorganisation of the SITCEN and Europol.

SITCEN

Although the fledgling Joint Situation Centre has only seven analysts, it deserves the label European intelligence agency since its function corresponds to that of an external intelligence agency. It is quite clear that the production of external intelligence could be ameliorated in both qualitative and quantitative terms if the centre was expanded and its system for tasking and control revised.

An expansion of the SITCEN is advisable both from an intelligence perspective and for political reasons. It is obvious that the level of staffing needs to be increased if the SITCEN is to serve the entire EU structure with the required support of situation and threat assessments. This is also necessary to allow the SITCEN to develop an intelligence capacity that surveys compliance with treaties that restrict armament, including non-proliferation treaties. An expanded SITCEN should include analysts from all member states. This would not only allow the centre to draw directly on the support of the national agencies from all member states; it would also do away with the political

[71] The quantitative and qualitative improvement of technical intelligence capabilities is largely a question of increasing spending and making research and development and procurement more efficient. For a detailed proposal on how procurement in general could be ameliorated within the EU, see Burkard Schmitt, 'The European Union and armaments. Getting a bigger bang for the euro', *Chaillot Paper* 63 (Paris: EU Institute for Security Studies, August 2003).

difficulty of explaining why the SGHR should obtain intelligence support from analysts seconded from seven, rather than from all member states. Even if the final SITCEN products are disseminated to all member states via the PSC, those states that are not represented in the centre do not have the same possibility to oversee and influence its work.

Modifications of the centre's tasking and control are necessary in order to ensure that situation assessments and those concerning man-made threats against EU field staff acting within the first pillar can be produced by the SITCEN when needed. The Commission's DG RELEX should therefore be able to task the centre. This issue would be solved automatically if the Convention's proposal of merging the roles of the SGHR and the Commissioner responsible for external relations were adopted. Meanwhile, a desirable solution to enhance cooperation between the SITCEN and EU field staff, and to enhance the centre's analysis capacity, would be for the Commission also to second personnel to the SITCEN, preferably persons from the DG RELEX with security clearance.

The current system with seconded analysts from national agencies, which is applied both in the INTDIV and the SITCEN, should be maintained and extended, so that national officers are double-hatted.[72] This system has two main advantages. First, national officers can be tasked by the EU structure while retaining their national competencies. Second, each state determines what access its national officer shall have to secret information, what powers he or she shall have to task national agencies and how they shall support him. Lengthy and hopeless negotiations on how the EU should be able to task national agencies could therefore be avoided.

Europol

Europol's ability to serve existing intelligence needs can easily be increased by a functional and geographical extension of its responsibilities. Giving Europol officers the possibility to participate in joint investigation teams has already had some positive effect.[73]

At present, Europol is only allowed to work on crimes where two or more member states are affected.[74] This means that it cannot scrutinise crimes that only affect a single member state, even if the criminal organisation is active in other non-member states. This becomes particularly odd when a criminal organisation is active in a crisis region where the EU is engaged. Today, activities of criminal organisations in such regions can only be the subject of Europol's efforts at the margin, at the request of local authorities, and provided the criminal organisations affect two or more of the Union's member states. Consequently, Europol cannot lend its expertise and act as an intelligence agency in support of e.g. Greece, FYROM, Albania and Serbia-Montenegro when dealing with organised crime in the region, unless another EU member state is affected by those criminal activities.

There are several reasons for extending Europol's mandate and various ways of doing it. To begin with, Europol should no longer be restricted to dealing with crimes that affect two or more member states. Since it is already dealing with transnational organised crime and terrorism,[75] it should be allowed to work with intelligence on criminal activities that extend from third states into a single EU state, especially from candidate states. It would have made sense if, for instance, Finland and Estonia (before becoming EU members) were given the option o f drawing on Europol's expertise, even

[72] This is also the case for Eurojust. Here, each Member State defines the nature and extent of the judicial powers it grants its national member of Eurojust. See Article 9(3) 2002/187/JHA. It should however be noted that Denmark was the only country that had clarified the competencies of its national member of Eurojust at the time of writing. According to Council of the European Union document 8740/02, 'Denmark's national member of Eurojust', the national member will not be competent to investigate and bring proceedings in criminal cases in Denmark, nor will he or she have competence as a judicial authority.

[73] 2002/465/JHA: Council Framework Decision of 13 June 2002 on joint investigation teams.

[74] Article 2 (1) of the Europol Convention.

[75] See Europol Convention Article 2.

if no other EU member was affected by the criminal activity in question. Lifting this restriction is also a prerequisite for the following three propositions.

Europol should survey crime in crisis areas that might pose a threat to existing or planned EU field missions, as the competency in the field of criminal and security intelligence can be needed to make adequate threat and situation assessments in support of the Union's external activities. To this end, Europol should submit such findings to, and interact closely with, the SITCEN. When necessary, Europol could even cooperate directly with EU field staff, e.g. with Union-led missions in the Balkans.

Furthermore, it could be tasked to develop an ability to take on the intelligence function for international police forces conducted by the Union itself or by other organisations, e.g. the UNMIK police.[76] This would allow Europol to support the production of security in 'failed states' at the same time as it gains experience in regions where criminal and terrorist organisations operate whose activities extend into the EU.

Finally, the Convention formulated suggestions adding the task of 'support[ing] action in combating terrorism at the request of a third country' to the Union's field of activities.[77] Here, Europol could be made responsible for intelligence support from the EU.

Such an extension of the EU's capabilities would give Europol unique functions. It would no longer duplicate the efforts of national agencies, and its customers would not be identical with the providers of intelligence. Europol could thus add more value, and the new accumulated knowledge might even have positive spillover effects on its intelligence support to authorities operating within the EU area.

Democratic supervision.

As the responsibility and capacity of EU agencies increase, the need for democratic supervision will become more pressing. This will particularly affect the SITCEN if it grows to become a veritable intelligence agency and extends beyond serving the SGHR. Until now, the SITCEN has been the only agency whose status has not been clarified in a legal document. It is important that this should be done soon. Rules regulating the tasking and control, as well as what each agency is allowed to do and how, must be determined. To pre-empt opposition to the development of EU agencies with reference to parliamentary prerogatives with a view to democratic scrutiny, regulations concerning supervision must also be determined. The purpose is not to complicate or limit cooperation between intelligence agencies. Rather, the aim is to simplify and possibly enhance it by giving legitimacy to it and moving it from a 'shadow' area into a clearly defined framework. The risk of EU agencies bringing pressure to bear on EU citizens is not particularly high, since the agencies do not have any operational functions. It is thus not very likely that European security would take priority over the defence of democracy and civil rights within EU agencies. Nevertheless, member states have to agree on a legislative framework to make sure that EU agencies cannot be used to bypass restrictions imposed upon national intelligence agencies by national law. This is for example important in the field of data protection. It should not for instance be possible for national agencies to transfer records to Brussels (or another member state which allows such registries) that they may not keep at the national level. Some kind of parliamentary committee should check compliance by EU agencies with these EU rules. The easiest solution would

[76] The international police force in Kosovo currently obtains support from the Central Criminal Investigation Unit (CCIU) set up by the United Kingdom, the United States, France, Spain and Italy.

[77] Article 17 of the European Convention, *Draft Articles on external action in the Constitutional Treaty*, CONV 685/03, Brussels, 23 April 2003. In the final Draft Treaty's Article III-210, however, this task was given less priority.

probably be to set up a joint committee composed of representatives from the national parliaments, or other bodies that control national intelligence agencies, and arguably, the European parliament.[78] Such a solution would underline the fact that EU agencies are accountable to member states and perhaps also, under special conditions to be agreed upon, the European Parliament. Similar suggestions have already been made for the scrutiny of Europol's work.[79]

7.2 Constructing a European intelligence communication network

At present, various national and EU agencies exchange intelligence on a bilateral level with some other agencies within the EU area. However, such contacts are not channelled through a common network that connects all agencies concerned within the EU area.[80] Even contact between EU agencies and national ones is conducted through bilateral channels. The establishment of a common network that allows all agencies to communicate with each other would facilitate the exchange of intelligence.

Counter-arguments are raised that such a 'technical tool' would not automatically enhance communications between agencies, since agencies still have to decide on utilising the network and on feeding information into it. Granted, there is no guarantee that the establishment of a European intelligence communication network would result in increased communication and cooperation among the interconnected agencies. However, two arguments support the idea that the network will be used and the exchange of intelligence increase.

First, and this is the weaker line of reasoning, one could draw a parallel with the development in other sectors. Is it too far-fetched to assume that the opportunities given to exchange information would have some influence on the way and the extent to which people within the intelligence community interact and communicate? It is well known that the establishment and extension of transport networks has led to an increase of traffic. Equally, nobody disputes the fact that the invention and institution of new communication networks, e.g. telephone, mobile phone and internet, have led to a revolution in, and increase of, long-distance communication between individuals.

The key argument, however, is that a European intelligence communication network would satisfy an existing demand and need to communicate. The necessity to exchange intelligence will remain whether or not there is such a network. The demand is thus induced by the threats, not by the existing means of communication. A limited exchange between agencies already exists, but it is unnecessary difficult and functions unsatisfactorily. This is not only a question of the parallel existence of various bi- and multilateral networks using different technologies and offering different options of communication. More important is the fact that no network interconnects all the agencies that need to cooperate in order to (a) fulfil their own task, and (b) allow for the production of the intelligence support needed by the EU. As a tool, the network will facilitate and boost secret communications and thereby improve the agencies' ability to produce and deliver the necessary intelligence support to their customers.

Increased intelligence exchange would have two main advantages. To begin with, it would improve the production of intelligence, i.e. the quality of threat detection and situation assess-

[78] For an overview of parliamentary supervision in some EU countries, see WEU Assembly Document A/1801, 'Parliamentary oversight of the intelligence services in the WEU countries – current situation and prospects of reform', submitted on behalf of the Committee for Parliamentary and Public Relations by Mrs Kestelijn-Sierens, Rapporteur, 4 December 2002. See also Les Documents de Travail du Sénat, 'Le contrôle parlementaire des services de Renseignement', *Série Législation Comparée*, no. 103, mars 2002.

[79] See House of Lords, Select Committee on the European Union, *Europol's Role in Fighting Crime*, 5th Report, Session 2002-2003. See also Communication from the Commission to the Council and the European Parliament, 'Democratic Control over Europol', COM (2002) 95 final, Brussels, 26 February 2002.

[80] The Club of Berne may be regarded as an exception, since they exchange some security intelligence through a common network.

ments. This is particularly true for EU agencies. Lacking sufficient collection, processing and analysis capacities they rely on intelligence provided by national services. Nevertheless, cross-agency and cross-border exchange of intelligence is also a prerequisite for the functioning of all other agencies, since none of them has the complete coverage required to handle its tasks.

Furthermore, a continuous sharing of intelligence between all agencies would enhance the chances of producing a common European response, i.e. for the elaboration and implementation of common European security policies. It is true that a network does not automatically result in a harmonised threat perception. However, facilitating communication increases the possibility that a common view is taken, and that countermeasures by various states and the EU are coordinated.

The question is how the contacts between agencies should be regulated and how a European network could be organised. As argued in section 6, the EU will not be able to, nor does it need to, regulate cross-agency and cross-border exchange among national services. However, it can facilitate communications, and must define the rules for EU agencies. To this end, a European intelligence communication network should be designed that somehow connects all EU and national agencies.

One must not be put off by the considerable technical and political challenges involved in the designing and setting up of such a network. It is quite clear that many attempts would be made to intercept communications transferred within it. Nevertheless, this is a problem that must and can be solved, as has been done with other networks. Such concerns should not be used as arguments to hinder the development and establishment of a secure common network, but rather to help define its standards.

Without getting lost in technical details, one can determine some general demands on such a network and formulate a few basic principles for its structure. A European intelligence communication network should interconnect all EU agencies and enable them to exchange intelligence with national agencies. If wisely structured, it might also provide a basis for the bilateral contacts between national agencies, and maybe even for exchanges at the national level. Furthermore, third states and organisations, most notably the United States, candidate countries and NATO, must be able to exchange information with the European intelligence community, and thus via the network. The network must allow for multi-media communication, at least in the form of voice, imagery, graphics and data.[81] It should also allow for instant messaging and have a ‘mail' function familiar to all e-mail users. This would include the possibility to attach files and steer dissemination with the equivalent of the Blind Carbon Copy (BCC) and Carbon Copy (CC) functions. Thereby all participants can exchange information selectively.[82]

For security reasons the network would have to be physically separated from other networks, and all communications would have to be encrypted. To limit access, especially in the case of intrusion, one could use firewalls within the wide area network and establish physically separated subnetworks. The latter would have a higher security level but at the price of speed and function. In this case, the exchange of information would have to take place by a physical transferral of storage medium, which means that instant messaging across that interface would not be possible and the exchange of intelligence slower.

Standardisation is a major challenge when designing such a network. This does not only concern technical specifications, but also classification and data protection regulations. Many of these standards must be agreed upon anyhow, in order to make exchanges with EU agencies possible.[83]

[81] It is quite clear that this requires a broad bandwidth. But, if the network is to add the expected value, this technical requirement must be met.

[82] NATO's BICES (Battlefield Information Collection and Exploitation System), which allows for such selective exchange, should be taken into account when developing this feature.

[83] Financing is another issue that has to be addressed. Irrespective of what technical standards are agreed upon, it is quite clear that the

When defining the methods, format and content of transmissions the EU should cooperate with third parties, most notably the United States, NATO and candidate countries. This would allow additional points of contact with the network to be established and exchange and cooperation with them to be enhanced. It is advisable to consider the US Defense Information Systems Network (DISN) and its two components for the transfer of sensitive and secret information (the Joint Worldwide Intelligence Communications System – JWICS and the Secret Internet Protocol Router Network – SIPRNET), when setting up a European network.

As mentioned earlier, some classification regulations have already been defined within the EU. If the standardised format and classification also applied at the national level, it would not only facilitate the international exchange, but also national exchange.

Data protection issues, finally, do not only concern time limits and other regulations on the storage of personal data.[84] It is above all a matter of the right of access to data and of its transmission, i.e. dissemination, along the following four types of path:

- from national agencies to EU 'agencies' and between national agencies;
- between EU 'agencies';
- dissemination from EU 'agencies' to other EU bodies and national authorities;
- between EU 'agencies' and third agencies (agencies of third states or other organisations).

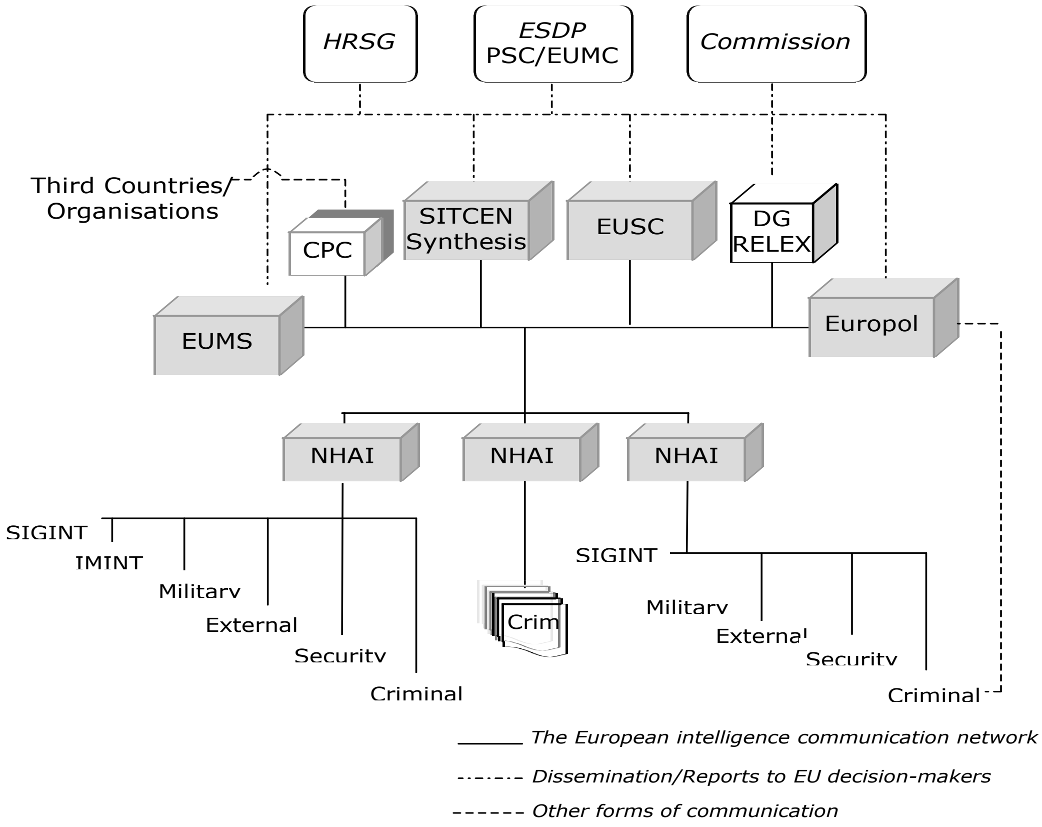

Figure 3: A European intelligence communication network

cost for setting up a European network will vary from state to state, depending on how far the system currently used at the national level is compatible with the new standards. It would be advisable to let the EU carry the costs of development, and to let it finance the network within the EU structure as well as to the 'capitals' of member states.

[84] Such rules already exist. According to Article 21 (3) of the Europol Convention, for instance, the time-limit on the storage of data by Europol is three years.

(a) This paper proposes the establishment of a European intelligence communication network that allows all EU intelligence agencies to exchange intelligence with a national point of contact in each country. The latter should not only have the status of a switchboard in the fashion currently applied by the European Judicial Network.[85] Ideally a 'National High Authority of Intelligence' (NHAI) would be set up in each country, and the point of contact located within it. If given responsibilities comparable to those of the Joint Intelligence Committee in the United Kingdom,[86] the NHAI could be in charge of both national and international intelligence coordination and cooperation. This does not mean that all contacts between EU agencies and national ones have to be controlled by the NHAI. Member states decide to what extent the network shall be utilised for exchanges among national agencies. Each country decides whether it shall have a physically separate national subnetwork, or if the national agencies shall be directly linked to the European network via the NHAI. Furthermore, it determines if the NHAI should have control over the international information flow through the network, or if the communication between national agencies and other points of contact within the network shall merely be channelled via the NHAI. Each country can also decide to maintain the established direct contact between national and EU agencies, e.g. between the INTDIV and national military intelligence services, and between Europol and national criminal and security agencies. However, in the long term integration into the system would be preferable, since this would facilitate the cross-border and cross-agency cooperation which is actually the whole point of the network. This is also why national analysts seconded to the SITCEN should belong to the national high authority. This would allow them to have a channel from 'above' into all national agencies.

(b) The relatively open flow of information between the current ESDP agencies (EUSC, SITCEN and INTDIV) should be maintained, although facilitated by the network. In addition, Europol should be connected to the second-pillar structure via the communication system. Regulations must be found to ensure that these Europol reports do not contain a level of detail that may jeopardise ongoing criminal investigations conducted by a member state or third countries. Since Europol is not responsible for any criminal investigations, it may be difficult for it to estimate in each single case what information may jeopardise prosecutions. Nevertheless, Europol officers are trained police officers and should be able to filter out too sensitive information from the reports, without nullifying their value added to the SITCEN. Seconding a Europol analyst to the centre could facilitate an adequate exchange. If, in the worst case, no general regulation can be found, the current practice for Europol's exchange with third countries may be applied for exchange with the ESDP structure.[87]

(c) Concerning dissemination from EU agencies, many current arrangements could be kept. The customers of EU agencies, i.e. the HRSG and Council units such as the PSC and the EUMC, do not need their own point of contact in the network. EU agencies will give these decision-makers the intelligence support they need in the form of final reports and analysis. Only the Commission should be linked to the

[85] See Article 2 (2) of Joint action 98/428/JHA. The points of contact can informally expedite requests for assistance in criminal prosecutions or investigations (so-called 'international judicial orders' or 'letters rogatory'). Once national authorities have obtained the necessary information and help from the point of contact, the communication concerning the actual judicial cooperation takes place directly between the competent authorities and outside the EJN.

[86] The tasks and responsibilities of the JIC are outlined on p. 19 in the second edition of the brochure National Intelligence Machinery published by the UK Stationary Office, 2001.

[87] See Article 18 of the Europol Convention. For a discussion on the transmission of data from Europol to third parties, see House of Lords, Select Committee on the European Union, *Europol's Role in Fighting Crime*, 5th Report, Session 2002-2003.

network, since it is also a main provider of intelligence. Its point of contact should be located in the part of DG RELEX, which has been cleared to handle secret information. It is imperative for intelligence cooperation that received intelligence is not spread further throughout the Commission. To exchange information with its missions abroad, the Commission could of course utilise the same technical equipment, but this should be a separate subnetwork. Decision–makers within the first pillar will thus be briefed selectively by DG RELEX or directly by EU agencies. Assessments of man-made threats to EU field staff, for instance, need only be available to those deciding on whether a mission should be launched or not. Only the equivalent of what in military terms is called 'force protection', e.g. information on what areas field staff should avoid and advice on how to behave, must be passed down to all personnel concerned. As for the dissemination from EU agencies to member states, the only modification needed would be that all ESDP agencies send copies of their products directly to the NHAI. Regarding Europol, the current dissemination procedures with the alterations addressed in the paragraph above could be maintained.

(d) The final point is far from the least important, and concerns the exchange of intelligence between EU 'agencies' and third parties, i.e. agencies of third states and other organisations. For obvious reasons, relations with the United States and NATO are very important. In the past, the EU has taken current NATO arrangements into account when organising the exchange of intelligence between the ESDP structure and the Alliance. When defining technical standards for the European intelligence communication network and intelligence standards, i.e. the form in which intelligence is to be transmitted, the Union must make sure that exchanges with NATO and the United States are not hampered. The best thing would be to let them and other third parties participate (have a voice, not a vote) in the preparatory discussions. Granting third parties direct access to the European network would, however, pose serious political difficulties. The EU intelligence community will not only be worried about external interception. Given the recent debate on Echelon it is quite clear that it would also be concerned with interceptions from within the network. Sharing the same physical network with non-members would therefore be highly controversial. To ensure that EU intelligence can be exchanged with third parties, one central point of contact (CPC) could be established in the network, or one such point within each EU agency. The latter would make it easier to maintain current arrangements for the exchange between the Union and the Alliance. The(se) CPC(s) would function as an interface(s) between physically separated networks with a physical transfer of storage medium between the two, as described earlier. If they wish, NHAI and national agencies could establish similar points of contact to communicate with third parties.

Conclusion

Taking the criteria of deliverability, feasibility, preservability and simplicity as a starting point, and considering those intelligence shortfalls identified in section 5 that can be redressed by organisational modifications, the study recommends the following alterations to the EU intelligence community:

First, the *SITCEN* should be expanded, with at least one seconded analyst from each member state, as well as representatives from the Commission and Europol. This would allow the centre to extend its current production of external intelligence, in particular assessments of threats against EU field staff. In addition, the centre should also begin to monitor compliance with treaties that limit armament.

Second, the competencies of *Europol* should be extended so that it can work on crime that only affects a single member state and a candidate or other state, at their request. It should also survey crime in crisis areas were the Union is or is planning on becoming active, and thereby contribute with its expertise to assessments made by the SITCEN. Furthermore, Europol should develop the ability to take on an intelligence function for international police missions.

Finally, the Union should set up a *European intelligence communication network* that connects all EU intelligence agencies with a central point of contact in each member state (ideally with a 'National High Authority of Intelligence'), or directly with national agencies. Through central points of contact, this physically separate network would also allow the exchange of intelligence with third parties. It would, therefore, not jeopardise any established intelligence relations, but rather facilitate the habitual cooperation and simplify the initiation of exchanges with new partner agencies.

Note that EU security policies would not be furthered by a merger of the existing EU intelligence agencies, or by a transfer of responsibility for the production of intelligence from the national to the European level. What the Union needs, and what it would obtain if the proposals made in this paper were adopted, are more powerful EU intelligence agencies characterised by greater cooperation with national ones.

This does not mean that greater cross-agency cooperation is not needed in Europe. Such an exchange is necessary for the production of accurate threat assessments, for developing methods that enhance the detectability of new threats as well as for sharing experience of their incidence. What the paper suggests is that this kind of cooperation between member states can largely be organised outside European institutions or 'heads', by the responsible national authorities. Current European institutions hardly need a more intense mix of cross-agency intelligence support than offered by the existing all-source external intelligence, which the SITCEN could deliver with the help of the various national and EU agencies.

At the national level, cross-agency cooperation could be managed by the NHAI in each member state. Through the European intelligence communication network, national authorities could then enhance their international cross-agency cooperation. Whether this takes place on a bi- or multilateral basis, if steered by the NHAI or if national agencies take direct contact with agencies in other countries, must be decided upon by each state and need not be regulated at the European level. A European intelligence communication system would facilitate such cooperation and coordination.

Annexes

Abbreviations

BCC	Blind Carbon Copy
CC	Carbon Copy
CFSP	Common Foreign and security Policy
CIS	Customs Information System
CPC	Central Point of Contact
DG	Directorate-General
ECHO	European Community Humanitarian Office
EIN	European Intelligence Communication Network
EJN	European Judicial Network
ESDP	European Security and Defence Policy
EU	European Union
EUMS	European Military Staff
EUSC	European Union Satellite Centre
FHQ	Force Headquarters
FYROM	Former Yugoslav Republic of Macedonia
HUMINT	Human Intelligence
IGO	Intergovernmental Organisation
IMINT	Imagery Intelligence
INTDIV	Intelligence Division of the European Military Staff
NATO	North Atlantic Treaty Organisation
NGO	Non-Governmental Organisation
NHAI	National High Authority of Intelligence
NIC	National Intelligence Cell
NILO	National Intelligence Liaison Officer
OLAF	European Anti-Fraud Office
OPHQ	Operational Headquarters
OSINT	Open-Source Intelligence
PPEWU	Policy Planning and Early Warning Unit
PSC	Political and Security Committee
RELEX	External Relations
SGHR	Secretary-General/High Representative of the EU
SIGINT	Signals Intelligence
SIS	Schengen Information System
SITCEN	Situation Centre
UAV	Unmanned Aerial Vehicle
UNMIK	United Nations Interim Administration Mission in Kosovo
US	United States
WEU	Western European Union
WMD	Weapons of Mass Destruction

Bibliography

Books and articles

- Andreas, Peter and Price, Richard 2001, 'From War Fighting to Crime Fighting: Transforming the American National Security State', in *International Studies Review,* No. 3, pp.31-52.
- Becher, Klaus, Molard, Bernard, Oberson, Fredric and Polti, Alessandro 1998, 'Towards a European intelligence policy', Institute for Security Studies Western European Union [Now European Union Institute for Security Studies], *Chaillot Papers,* No. 34, Paris. Available at: http://www.iss-eu.org/.
- Betts, Richard 2002, 'Fixing Intelligence', in *Foreign Affairs*, Vol. 81, No. 1, pp. 43-59.
- Bruneau, Thomas 2001, 'Controlling Intelligence in New Democracies', in *International Journal of Intelligence and Counterintelligence*, Vol 14 , No 3, pp. 323-341.
- Grant, Charles 2000, 'Intimate Relations: Can Britain play a leading role in European defence – and keep its special links to US intelligence?', *CER working paper*.
- Hagman, Hans-Christian 2002, 'European Crisis Management and Defence: The search for Capabilities', in IISS, *Adelphi Paper*, No. 353.
- Hastedt, Glenn 1991, *Controlling Intelligence*, London.
- Heisbourg, François (ed.) 2000, 'European Defence: making it work', in *Chaillot Papers*, no. 42.Herman, Michael 1995, 'Intelligence After the Cold War: Contribution to international Security?', *Brassey's Defence Yearbook*, pp. 369-383.
- Herman, Michael 1998, 'Diplomacy and Intelligence', in *Diplomacy & Statecraft*, Vol. 9, No. 2 (July), pp. 1-22.
- Hermann, Michael 2001, *Intelligence Services in the Information Age. Theory and Practice*, London.
- Hoffman, Bruce 1996, 'Intelligence and Terrorism: Emerging Threats and New Security Challenges in the Post-Cold War Era', in *Intelligence and National Security*, Vol. 11, No. 2, pp. 207-223.
- International Crisis Group (ICG) 2001, *EU crisis Response Capability: Institutions and Processes for Conflict Prevention and Management*, Brussels.
- International Crisis Group (ICG) 2002, *EU Crisis Response Capabilities: An update*, Brussels.
- Knightley, Phillip (1988), *The second oldest Profession: Spies and Spying in the twentieth century*, New York.
- Lange, Hans-Jürgen 1999, *Innere Sicherheit im Politischen System der Bundesrepublik Deutschland*, Opladen.
- Müller, Harald 2003, 'Terrorism, proliferation: a European threat assessment', in EUISS, *Chaillot Papers*, No. 58.
- Müller-Wille, Björn 2002, 'EU Intelligence Co-operation A critical Analysis', in *Contemporary Security Policy*, Vol. 23, No. 2 (August).
- Müller-Wille, Björn 2003, *Thinking Security in Europe – is there a European Security and Defence Identity,* Münster. Available at: http://miami.uni-muenster.de/servlets/DerivateServlet/Derivate-1012/.
- Pullinger, Stephen and Quille, Gerrarad 2003, 'The European Union: Tackling the threat from Weapons of Mass Destruction', in ISIS Europe and Safeworld*, Discussion and Policy Papers*.
- Ransom, Harry 1970, *The Intelligence Establishment*, Cambridge.
- Richelson, Jeffrey 1995, *A Century of Spies: Intelligence in the Twentieth Century*, Oxford.
- Shulsky, Abraham 2002, *Silent Warfare: Understanding the World of Intelligence*, third edition, Washington, D.C.
- Statewatch 2002, *SIS II takes ominous shape,* 4 April.
- Thuillier, François 2000, *L'Europe du secret : mythes et réalité du renseignement politique interne*, Paris.
- Warner, Michael 2002, 'Wanted: A Definition of Intelligence', in *Studies in Intelligence*, Vol. 46, No. 3. Available at: www.cia.gov.
- Wijnen Reims, Joy 2002,'Historical Overview: National Security Service (BVD) to General Intelligence and Security Service (AIVD)', *DCAF Conference Paper*.
- Villadsen, Ole R 2000, 'Prospects for a European Common Intelligence Policy', in *Studies in Intelligence*, Vol 44, No. 9. Available at: www.cia.gov.
- Zegart, Amy 1999, *Flawed by design: the evolution of the CIA, JCS, and NSC*, Stanford.

Official documents

- *A secure Europe in a better world. European Security Strategy* - approved by the European Council held in Brussels on 12 December 2003 and drafted under the responsibilities of the EU High Representative Javier Solana.
- COM (2002) 95 final: Communication from the Commission to the Council and the European Parliament, *Democratic Control over Europol*, Brussels 26 February 2002.
- COM (2002) 233 final: Communication from the Commission to the Council and the European Parliament, *Towards integrated management of external borders of the Member States of the European Union*, Brussels 7 May 2002.
- Congressional Research Service (CRS) Report for Congress, *Homeland Security: Intelligence Support*, Updated 4 March 2003, RS21283.
- Council of the European Union 2002, Document 8740/02, *Denmark's national member of Eurojust,* Brussels 8 May.
- Council of the European Union 2003, *Press Release*, 'European defence: Nato/EU consultation, planning and operations', Brussels 15 December.
- European Convention, *Draft Articles on external action in the Constitutional Treaty*, CONV 685/03, Brussels 23 April 2003.
- European Convention, *Draft Treaty establishing a Constitution for Europe*, CONV 850/03, Brussels 18 July 2003.
- European Council Santa Maria da Feira, *Presidency Conclusion*, 20 June 2000.
- European Council Göteborg, *Presidency Report*, 16 June 2001.
- European Council Thessaloniki, *Presidency Conclusion*, 20 June 2003.
- House of Commons, Foreign Affairs Committee, The Decision to go to War in Iraq, 9th Report, Session 2002-03.
- House of Lords, Select Committee on the European Union, *Europol's Role in Fighting Crime*, 5th Report, Session 2002-2003.
- House of Lords, Select Committee on the European Union, *EU – Effective in a Crisis?*, 7th Report, Session 2002-3.
- IGC 2003, Document CIG 57/1/03, Brussels 5 December.
- IGC 2003, Document CIG 62/03, Brussels 5 December.
- IGC 2003, Document CIG 60/03 ADD 1, Brussels 9 December.
- Informal General Affairs and External Relations Council (Gymnich), 2-3/5/2003: *Statements by Foreign Minister G. A. Papandreou*, Rhodes, 2/5/2003. Available at http://www.eu2003.gr/en/articles/2003/5/2/2659/.
- Les Documents de Travail du Sénat, 'Le contrôle parlementaire des services de Renseignement', *Série Législation Comparée*, No 103, March 2002.
- The National Security Service (BVD), *Annual Report 2001*.
- The Stationery Office 2001*, National Intelligence Machinery,* second edition. Available at: http://www.official-documents.co.uk.
- U.S. House of Representatives, One Hundred Fourth Congress, Staff Study Permanent Select Committee on Intelligence, *IC21: The Intelligence Community in the 21st Century*, 1997. http://www.access.gpo.gov/congress/house/intel/ic21/index.html.
- WEU Assembly Document A/1775, *The new challenges facing European intelligence – reply to the annual report of the Council,* Submitted on behalf of the Defence Committee by Mr Lemoine, Rapporteur, 4. June 2002.
- WEU Assembly Document A/1801, *Parliamentary oversight of the intelligence services in the WEU countries – current situation and prospects of reform*, submitted on behalf of the Committee for Parliamentary and Public Relations by Mrs Kestelijn-Sierens, Rapporteur, 4 December 2002.
- White House Fact Sheet, 'Strengthening Intelligence to Better Protect America', 28 January 2003.

Legal documents

- Schengen Convention – Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders.
- Europol Convention – Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office. OJ C 316, 27 November 1995.
- Council Regulation (EC, Euratom) No 2988/95 of 18 December 1995 on the protection of the European Communities financial interests.
- 96/277/JHA: Joint Action of 22 April 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning a framework for the exchange of liaison magistrates to improve judicial cooperation between the Member States of the European Union.
- 1257/96/EC: Council Regulation of 20 June 1996 concerning humanitarian aid.
- 98/428/JHA: Joint action of 29 June 1998, adopted by the Council, on the basis of Article K.3 of the Treaty on European

Union, on the creation of a European Judicial Network.

- Council Regulation (EC) No 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF).
- 2001/80/CFSP: Council Decision of 22 January 2001 on the establishment of the Military Staff of the European Union.
- 2001/555/CFSP Council Joint Action of 20 July 2001 on the establishment of a European Satellite Centre.
- 2001/792/EC: Council Decision of 23 October 2001 establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions.
- 2002/187/JHA: Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime.
- 2002/465/JHA: Council Framework Decision of 13 June 2002 on joint investigation teams.

Websites

▮ http://www.fas.org	Federation of American Scientists
▮ http://www.geheimdienste.org	

Occasional Papers

All *Occasional Papers*
can be accessed via the Institute's website:
www.iss-eu.org

n° 49	EU cohesion in the UN General Assembly *Paul Luif*	December 2003
n° 48	Space and security policy in Europe: Executive summary *Stefano Silvestri, Rapporteur*	December 2003
n° 47	EU and Ukraine: a turning point in 2004? *Taras Kuzio*	November 2003
n° 46	EU-Russian security dimensions *Edited by Dov Lynch*	July 2003
n° 45	€uros for ESDP: financing EU operations *Antonio Missiroli*	June 2003
n° 44	The Galileo satellite system and its security implications *Gustav Lindström with Giovanni Gasparini*	April 2003
n° 43	La question du Cachemire. Après le 11 septembre et la nouvelle donne au Jammu et Cachemire *Christophe Jaffrelot et Jasmine Zérinini-Brotel*	Mars 2003
n° 42	L'Union en action : la mission de police en Bosnie *Agnieszka Nowak*	Janvier 2003
n° 41	La Bulgarie et la Roumanie dans le Pacte de stabilité *Ralitza Dimtcheva*	Janvier 2003
n° 40	Iraq: a European point of view *Martin Ortega*	December 2002
n° 39	Iraq: the transatlantic debate *Philip H. Gordon*	December 2002
n° 38	Getting there: building strategic mobility into ESDP *Katia Vlachos-Dengler*	November 2002
n° 37	From candidate to member state: Poland and the future of the EU *Rafal Trzaskowski*	September 2002
n° 36	Optimiser le processus de Barcelone *Dorothée Schmid*	Juillet 2002
n° 35	L'ONU au Kosovo : leçons de la première MINUK *Eric Chevallier*	Mai 2002
n° 34	Bigger EU, wider CFSP, stronger ESDP? The view from Central Europe *Edited by Antonio Missiroli*	April 2002
n° 33	A new European Union policy for Kaliningrad *Sander Huisman*	March 2002
n° 32	Managing separatist states: a Eurasian case study *Dov Lynch*	November 2001