CHAPTER FIVE
Intelligence cooperation in the European Union

Major-General Graham Messervy-Whiting, Centre for Studies in Security and Diplomacy, University of Birmingham [1]

INTRODUCTION

Before the year 2000, there was virtually no intelligence cooperation[2] within the institution of the European Union. There were, of course, vigorous networks of both bilateral and multilateral intelligence cooperation, throughout the continent of Europe, between states. National intelligence agencies have always had dealings with combinations of their peers – combinations which have depended on principles such as identified long-term and short-term common interests, trust and reciprocity. The depth of this cooperation has varied not only between states but also between the various intelligence disciplines. For example, the human intelligence (HUMINT) agency of State A might have a particularly close professional relationship with the HUMINT agency of State B, whereas the signals intelligence (SIGINT) agency of the same State A might be closer to the SIGINT agency of State C. Within the field of defence-related intelligence, there was also a highly formalised system of intelligence cooperation within the NATO alliance, mainly in the field of threat assessment, and driven until the 1990s by the needs of the Cold War.

1. The views expressed in this paper are the author's alone.
2. This chapter covers intelligence cooperation in the fields of foreign and security policy and defence at the politico-strategic level. It does not seek to cover cooperation below this level, nor other forms of intelligence cooperation, such as in the fields of Justice and Home Affairs.

Defence intelligence cooperation within the institution of the EU started in the year 2000 as part of the development of the ESDP dossier, which was given impetus by the 1999 Helsinki meeting of the European Council.[3] By 2003, a system for such cooperation had not only been designed and the design endorsed by all the principal stakeholders, but a brand-new multinational and multi-service ('combined joint' in military-speak) intelligence staff was also up, running and producing intelligence for its entire range of customers. Broader intelligence cooperation in the domain of foreign and security policy followed hard on defence's heels. It is important to make it clear up front that we are not referring here to any creation of an 'EU intelligence service', in the same way that the ESDP initiative has not led to any creation of an 'EU Army', 'Navy' or 'Air Force'. What the EU has developed is a system for delivering a high-quality EU intelligence product, fused from national and some non-national contributions, to its CFSP/ESDP customer base.

The backdrop to these developments included the fact that the EU's politico-military structure had started to take on flesh in the autumn of 1999 in the Justus Lipsius building, the EU Council's main building in Brussels, with the arrival of Dr Javier Solana as the first Secretary-General/High Representative, of Pierre de Boissieu as the Deputy Secretary-General, and of the first members of the Policy Planning and Early Warning Unit, now known simply as the Policy Unit. In early 2000, the interim Political and Security Committee and the Military Committee held their first meetings, and the design for a brand-new military directorate-general was completed, being officially approved by the end of that year. By spring 2001, an EU Military Staff was forming up and moving from the Justus Lipsius building to the purpose-adapted Kortenberg building some seven hundred metres away. It did so not alone but along with all its key non-military colleagues in the EU's politico-military structure, such as the bulk of the Directorate-General for External Affairs, the Policy Unit and the Joint Situation Centre (SITCEN). By the end of 2001, the Political and Security Committee and the Military Committee had ceased to be

3. For more details about the background to this development, see Björn Müller-Wille's well-informed article, 'EU Intelligence Cooperation. A Critical Analysis', in *Contemporary Security Policy*, vol. 23, no. 2, August 2002.

'interim' and had taken their place as official Council bodies, while the EU Military Staff had been declared as having attained 'full staff capability', i.e. the capability of carrying out all aspects of its mission statement.[4] The year 2002 saw all elements of the politico-military structure beginning to work together effectively and productively; the development of a large number of concepts, policies and procedures, including a handbook of crisis-management procedures; the EU's first-ever crisis-management exercise, CME 02; the launch of an EU police mission in Bosnia; and the watershed of a long-awaited agreement between the EU and NATO on 'Berlin-plus'. By spring 2003, the EU had launched its first-ever military operation, Operation Concordia, in the former Yugoslav Republic of Macedonia – an operation with recourse to NATO assets and capabilities – and, by summer 2003, its second military operation, Operation Artemis, in Ituri Province of the Democratic Republic of Congo – an operation without recourse to NATO.

This chapter seeks to outline how the rapid turnaround in intelligence cooperation was achieved, looking at some of the driving design factors, some of the key enabling factors and the development of intelligence product, before offering some thoughts for the future.

Throughout this chapter, as indicated in italics, a mythical EU-led peace support operation (Operation Zeus) in a fictitious coastal West African country in the year 200X will be used to illustrate some of the more technical points. The EU decided to launch Zeus, following an appropriate UN Security Council Resolution, as a short, sharp, rapid-reaction operation to secure and stabilise the principal entry points to the country and its capital, prior to the arrival of a larger UN force with a broader and longer-term mandate. The UK's offer to the EU to be the 'framework state' for this operation was

4. See below under 'Treaty provisions'. The EU Military Staff, at around 130 people, including support staff, is approximately half the size of NATO HQ's International Military Staff (IMS).

accepted. The operation's headquarters (HQ) was therefore to be the UK's Permanent Joint HQ (PJHQ Northwood); the EU Operation Commander and the commander of the deployed forces were to be British. The UK would provide the bulk of the forces, from a carrier group already positioned over the horizon off the West African coast, with aircraft from the UK, France[i] and Spain and also elements of UK and French 'battle groups'[ii] already embarked. Offers of military capability from a total of eighteen EU member states were accepted, as were offers from four non-EU countries. Most member states' offers included individual reinforcements to multinationalise the operation and Force HQ Staffs. Non-EU countries' offers included airlift, communications and intelligence capabilities.

i) Persuant to the Le Touquet summit agreement of February 2003

ii) Persuant to the French/German/UK 'food for thought' paper presented to the PSC on February 18th 2004

SOME DRIVING DESIGN FACTORS

The Customer is King

The primary objective of any intelligence system should be to provide what the customers need in a timely and user-friendly format. In the EU's case, the principal customers are the actors in the politico-military decision-making process. These include the EU Military Committee and the Political and Security Committee; the High Representative; other in-house Council actors, such as the Directorate General for External Affairs and the Policy Unit; the Commission; and, during an EU-led crisis-management operation, the chain of command. No single customer from amongst this list is invariably more or less important than any other: priorities vary according to the stage reached in the decision-making process, who is about to do what, and whether there is an operation in progress.

In so far as military operations are concerned, the EU Military Committee (EUMC) is a vital piece of the EU's politico-military machinery. Meeting at its most senior level, it is composed of the Chiefs of Defence of the member states. The normal format of the EUMC is the Military Representative level, consisting of senior Brussels-based General/Flag Officers representing their Chiefs of Defence. It is the EUMC which delivers to the EU decision-making machinery the unanimous advice of the Chiefs of Defence on all military matters. Experience quickly showed that the most efficient way to deliver intelligence product to this customer was through short, sharply focused audio-visual briefings at the beginning of the relevant agenda items, coupled with the dissemination of written reports, wherever possible delivered in advance by electronic means to the Brussels-based delegations.

The political control and strategic direction of EU-led operations can now be delegated by ministers direct to the Political and Security Committee (PSC), which takes its input on military issues from the EU Military Committee and, on non-military issues, from the Committee for Civilian Aspects of Crisis Management. As with the Military Committee, experience quickly confirmed that even shorter, sharper audio-visual presentation was the most effective way of providing key intelligence product.

The High Representative is both the principal in-house customer for intelligence product and, it proved, one of the most challenging to service. Solana's high-level and worldwide political activity was both hectic and subject to change at very short notice. His main needs proved to be quick, preferably verbal readouts at short notice.[5] Face to face contact in Brussels was preferred, but inevitably, telephone or e-mail contact at a greater distance often proved necessary.

5. For example, the first intelligence request that Solana passed to the author was in April 2000 for basic information about the terrorist organisation which at that time was holding some EU citizens hostage in the Philippines. Solana had learnt a few minutes earlier that the member states had agreed that he should fly the following day to represent the EU position on this issue personally to the President of the Philippines. A quick answer, derived from open sources, was delivered verbally within thirty minutes. During a stopover en route, Solana received by hand from a representative of one member state hard copy of a product compiled from classified material.

The Directorate-General for External Affairs had always dealt with foreign affairs issues for the Council and was organised on a classic regional directorate basis, together with certain directorates dealing with cross-regional issues. It was authorised – fairly late in the day compared to the other in-house teams – to recruit a slim, additional 'pol-mil' directorate, which started to develop a critical mass in late 2001. The main task of the Policy Unit was to provide forward thinking on foreign and security policy issues for the High Representative, but it also became drawn into expeditionary, hands-on diplomacy in the EU's high-priority areas of concern, such as the Balkans and the Middle East. For both these in-house actors, the main requirement was to be able to exchange working-level information and to network on a continuous basis, both face to face and by electronic means.

The Commission, and in particular its recently created External Affairs Directorate-General, was, both *de facto* and *de jure*, a vital player in the EU's overall politico-military structure. However, at the time of writing, its contribution across the structure has not yet fully matured, partly for reasons of residual intra-institutional 'turf protection' between the EU's first pillar (Commission) and second pillar (Council Secretariat) actors. Its main customer need was similar to that of the in-house Council actors, but with the disadvantage of a lack of collocation. Where face-to-face networking was not possible, a less than satisfactory recourse to the transmission of hard-copy product had often to be made.

For the operation commander and his headquarters during an EU-led operation, the challenge was not only to provide him with 'top-down' intelligence but also to design a system to ensure that the intelligence staffs all the way down the command chain received directly all the available feeds they needed and were also alive to what needed to flow 'bottom up'. In other words, once an EU-led force was deployed to the area of operations, the command chain became not only a customer but also a prime source of intelligence input to the EU's politico-strategic level. The ideal solution to these needs was the acquisition of a web-based system; until such time as this became feasible, secure IT and communications links, including a videoconferencing facility, were an absolute necessity.

Treaty provisions

What the EU can and cannot do is governed by the Treaty of the European Union. Another driving design factor was therefore what the Treaty had to say about the CFSP and ESDP. The former is mainly covered by Article 11 which, amongst other things, talks to: safeguarding the fundamental interests, independence and integrity of the Union; strengthening the security of the Union in all ways; and preserving peace and strengthening international security. ESDP is covered principally by Article 17, which includes references to the progressive framing of a common defence policy, and the Petersberg tasks including humanitarian and rescue missions, peace-keeping, and the use of combat forces in crisis management, including peacemaking. Thus the Treaty provided a solid basis for a global, holistic approach to the design of the EU's intelligence architecture. The main rules governing this design were the EU Military Staff Terms of Reference. These had the status of a Heads of State and Government-level (European Council) decision and included the Military Staff's mission, function and outline organisation. The mission included the tasks of early warning, situation assessment and strategic planning in relation to the potential Petersberg missions. These tasks clearly pointed towards a proactive, robust and effective defence intelligence component.

The intelligence cycle

The intelligence cycle of activity includes the main steps of collection, collation, interpretation, assessment, dissemination and system feedback. The EU decision-making machinery's prime need is for assessed intelligence, the steps of collection, collation and interpretation being part of the spectrum of capabilities offered to the EU by the member states. The main exceptions to this were that some collation and interpretation would also be available, in the imagery intelligence (IMINT) field, from the EU's Satellite Centre Agency at Torrejon; and that, during an EU-led operation, the chain of command would, in the theatre of operations, be engaging in the entire intelligence cycle of activity, with the intelligence, surveillance, target acquisition and reconnaissance (ISTAR) assets being made available by the participating states.

To illustrate these two exceptions, at an early stage in the run-up to the decision to mount the fictitious Operation Zeus, the EU Military Staff had made a number of task requests to the Satellite Centre for up-to-date imagery coverage of the likely theatre of operation, at a scale of 1:50,000, and for more detailed coverage of several key points, such as the main port and airfield. The Satellite Centre had bought in some high-grade, commercially available Russian and US satellite imagery, some of which was only three months old. Its analysts had had time to do some quick interpretation of routes and obstacles around the airport area. Once the EU Council had decided to launch Operation Zeus, aircraft from the carrier group started to over-fly the area of operation and provide the operation commander with some up-to-the-minute images. Small teams of special forces were inserted near some of the key points to provide some continuous, real-time de visu Human Intelligence. One specially equipped vessel also deployed covertly close inshore to gather Signals Intelligence against targeted low-power/short-range voice circuits.

The need for a joint assessment process[6] was another key driving design factor. One of the Policy Unit's officials had been instrumental in getting the EU Council's interim Situation Centre up and running. During 2002, the Joint Situation Centre developed from being co-led by the Policy Unit and the EU Military Staff into being directed by one full-time official working for the High Representative. The primary purpose of this development was to create the conditions whereby member states' non-military intelligence agencies could feel comfortable enough to contribute selected intelligence product to the EU via the Situation Centre. The defence intelligence organisations of the member states had, in 2000, already agreed to do this for selected military intelligence product via the Intelligence Division of the Military Staff. In 2003, the Joint Situation Centre was

6. The term 'joint' in this context refers to the coming together of the relevant military and non-military components.

also developed to provide the platform for the twenty-four hour monitoring of the EU's current operations and for the presentation of a coherent package of briefings for all customers on current situations around the world.[7]

There was also a need to situate the intelligence function firmly within an overall information management architecture for the EU and not to let it operate as some separate, stand-alone entity. To this end, the EU Military Staff quickly drafted not only a military information operations concept, but also encouraged the EU Council General Secretariat to design an overarching information management concept paper, subsequently issued in September 2001.

Benchmarking

Another driving design factor was the desire – given the luxury of a virtually 'clean-sheet' opportunity to design the best possible achievable intelligence system by benchmarking against the best existing systems in the member states – international organisations and non-governmental organisations, taking the best elements from each and leaving the least best behind.

SOME KEY ENABLING FACTORS

It was quickly evident that the key internal stakeholders, who controlled all the main management tools, such as the release of finance, personnel policy, the allocation of office space and policy for IT and Communications and other major equipment projects, had to be brought on board. They were indeed, and it was mainly thanks to them that the intelligence cooperation function was able to take its place so quickly in the overall EU Council structure.

7. For more detail, see the UK House of Lords 7th Report of the Select Committee on the EU (*HL Paper* 53, dated February 11th 2003), pp. 15-19.

One of the first key decisions was to give all aspects of security, including the need for modern, secure IT and communications, the high priority required to gain the confidence of key external stakeholders that what they put into the EU's intelligence system would be safely looked after. It was decided that the cast of CFSP/ESDP 'workers', including all those engaged in the intelligence function, should be moved to the purpose-adapted Kortenberg building. In doing so, the disadvantage of being some seven hundred metres away from face-to-face contact with many of the key in-house customers in the Justus Lipsius building was accepted. The first visit of the Military Staff design team and of security experts to the Kortenberg took place in April 2000. By May 2001, adaptation of the building had been largely completed and the 'workers' were moving in. In between, in July 2000, another key enabling factor – the interim security agreement between the EU and NATO – had been signed. An overarching communications and information systems concept was quickly drafted and, by December 2001, had been accepted by all the stakeholders, being 'noted' by the Political and Security Committee. The long-range vision was of a 'web-pull' of information over a secure wide-area network, with the bandwidth to permit a secure videoconferencing facility. The short to medium-term vision was to adapt what was currently available to build various layers or 'onion rings' of systems. Thus a secure local-area network was quickly designed for the whole Kortenberg CFSP/ESDP community, and a separate, stand-alone, secure intelligence local-area network designed for the defence intelligence function within this community. The first terminals were delivered in October 2001, and interim system accreditation was achieved in January 2002. Informal discussion was launched with NATO's BICES[8] Agency in April 2000. After much debate between member states, the detailed requirement was accepted by EU stakeholders and formally put to the BICES Agency in March 2003. Videoconferencing trials with existing equipment and bandwidth were successfully carried out in late 2001 and early 2002 with two of the potential operational headquarters (UK and France); its first operational use was in March 2003, when the

8. BICES is a secure, web-pull system for the distribution of defence intelligence, mainly but not exclusively between NATO nations.

Political and Security Committee came to the Joint Situation Centre to conduct a live dialogue with the EU Police Mission Commander in Sarajevo.

The key external stakeholders were the Chiefs of the Defence Intelligence Organisations (CDIs) of the member states, without whose full support no system of effective EU defence intelligence cooperation could work. Informal bilateral discussions with them were started in July 2000, with a first low-key 'conclave' of CDIs being held in Brussels – though not in an EU facility – in September 2000. By November 2002, the fourth such conclave was being held in an EU building and was attended, for part of the time, at least, by Solana. Conferences with all the potential elements of the EU's chain of command for military operations were begun in December 2001, informal contacts with NATO headquarters, SHAPE and UN headquarters in New York having already been started from August 2000 onwards. Every effort was made, from Solana downwards, to keep the US administration and its intelligence agencies accurately informed as to what the EU was doing in this field throughout the design phase, with the first high-level Department of Defence visitor being briefed in Brussels as early as March 2000.

Within the vital field of the development of the EU's military capabilities to achieve the Helsinki Headline Goal, in 2002 equipment capability action panels started focussing on challenging intelligence-related capability needs, such as strategic-level IMINT, SIGINT, early warning and distant detection, and battle damage assessment and in-theatre surveillance and reconnaissance (to pull together 'recognised land, sea and air pictures'). In parallel, a military intelligence, surveillance, target acquisition and reconnaissance (ISTAR) concept for EU-led operations was quickly worked up and issued in November 2001.

THE DESIGN TAKES SHAPE

So, having pulled all these factors together, the presentation given to that very first conclave of CDIs in September 2000 outlined the need for an Intelligence Division (INT), where the personnel would be seconded to the EU Military Staff, normally

for a tour of duty of three years, from their defence intelligence services. In other words they would, wherever possible, be intelligence professionals and would be provided with a secure IT and communications link back to their national service. The EU in its turn would provide each of them with a secure room which, in addition to meeting the EU's security standards, could also be adapted to meet any additional national security criteria. INT's mission would be centred on the Military Staff's core tasks of early warning, situation assessment and strategic planning. INT would be organised into three branches: a small branch dealing with policy issues; another small branch dealing with requirements issues in the main intelligence disciplines; and a large production branch to produce and deliver the intelligence to the customers. Production would be organised into the same four geographic groupings as the other main actors in the EU politico-military structure, namely the Balkans; the Middle East and Africa; countries to the east of Europe; and the rest of the world. Product would, in descending order of preference, be web-based, audio-visual, verbal and – only where none of these means were possible or appropriate – in hard paper copy. INT would be empowered, as tasked by the Director-General of the EU Military Staff, to take the initiative in studying and reporting on a particular issue – in other words, it could act or react quickly to new developments. It would also maintain a small 'front-end cell' in the Joint Situation Centre to act principally as INT's feed to and from a joint assessment process and, during operations, into and out of the monitoring of the operational situation. From the start, great emphasis was laid on the need for high-quality personnel to be assigned to INT by the member states. While the four top posts (division and branch heads) were to be open for any member state to bid for, an equitable spread of the working-level posts between the member states was agreed, which also played to the particular strengths of each national Defence Intelligence Organisation (DIO). For example, officers from Austria, Greece and Italy were assigned to posts covering the Balkans and officers from Finland and Sweden to 'east of Europe' posts. INT would be provided with a secure, stand-alone local-area network, equipped with excellent internal search facilities, which would be the default means of handling all elements of its intelligence processing functions. The member state DIOs would be asked to provide INT in response to a regularly updated and agreed 'global overview' watch list, with periodic assessed intelligence

product (not raw data), which would, wherever possible, be pre-sanitised for release 'at fifteen', in other words to all the member states. They would also be asked to respond to specific questions from INT,[9] particularly during crisis management or an EU-led operation. A very important principle adopted from the very beginning was that all member state DIOs would, in turn, receive copies of all INT's intelligence reports.

The Chiefs of Defence Intelligence at that first conclave gave an informal 'green light' for this design to be put into effect. The first secure IT and communications link was established in May 2001, shortly after the move into the Kortenberg facility. By the summer of 2002, fourteen out of the fifteen member states' DIOs had established such links, and fourteen were providing defence intelligence already pre-sanitised to enable its release to all fifteen. Non-national inputs included open sources of information (OSINT), from contracts entered into with four civilian firms from November 2001 onwards; geographical information (GEO) from the GEO specialist of the EU Military Staff; and IMINT from the EU Satellite Centre. The OSINT strand was developed after consultation in particular with the Swedish DIO, one of the world leaders in this field. A first conclave of GEO experts from the member states was held in February 2002, leading to the establishment of an EU Military Staff GEO database in October 2002. Initial informal contacts with what was then the WEU Satellite Centre started as early as April 2000, the first product coming on line soon after the Centre officially became an EU agency in 2001.

INT, as an integral part of the EU Military Staff, played its full part in the internal training programme leading to the declaration, in December 2001, that 'full staff capability' had been achieved, as well as in the development of the EU's first-ever crisis-management exercise in June 2002. But its progress can perhaps best be measured by looking at some of the milestones in the EU's intelligence product, resulting from both the military assessment process, then the development of joint assessment in the Kortenberg facility. The first product – not strictly speaking an intelligence one, but nevertheless a test product of the interim Joint Situation

9. So-called 'Requests For Information' or RFIs.

Centre, which was still then located in the less than fully secure Justus Lipsius building – was a joint 'press summary' which started in December 2000. The EU Council's press office was, of course, already producing press summaries for its senior customers, but the Situation Centres product was in effect a periodic open source intelligence summary tailored for its developing CFSP/ESDP customer base.[10] In March 2001, the developing Intelligence Division started a test periodic 'military highlights' summary tailored for the same customer base and again derived from open sources.[11] The move to the Kortenberg was accompanied by the first test audio-visual presentation by INT of a military intelligence report (INTREP),[12] on a current situation, to an internal Council General Secretariat audience headed by the Deputy Secretary General. This was quickly followed, in July 2001, by the first audio-visual intelligence briefing,[13] to the EU Military Committee. The Joint Situation Centre produced its first periodic joint intelligence summary, at that stage derived from open source intelligence alone, in September 2001.[14] The Chairman of the EU Military Committee came to INT for the first time in October 2001 to receive a classified audio-visual briefing;[15] the first SECRET-level intelligence report was produced by INT later that month for senior in-house customers, necessarily, at that stage, in hand-carried hard-copy format. November 2001 saw the first of what then became the regular classified audio-visual INT briefings to each meeting of the Military Committee. By January 2002, INT had given its first 'early-warning hotspots' presentation, and also,

10. For example, items would be grouped under regional headings, such as: the Balkans, Middle East, East of Europe, Africa, Asia and the Americas.

11. Items would again be grouped under regional headings, but focus on armed forces highlights, such as the introduction of a new weapons system in the armed forces of a Middle Eastern country, or the latest assessment of the military situation in a sub-Saharan country.

12. An INTREP focuses on one particular item of intelligence, normally adjudged to be of high enough value and time sensitivity to warrant separate reporting in advance of the next periodic (e.g. weekly) intelligence summary (INTSUM), a round up normally grouped under regional and/or topic headings.

13. It was on the situation in the former Yugoslav Republic of Macedonia (fYROM).

14. It was, coincidentally, put out on 9/11, and included, under the topic of global terrorism, a paragraph on the generic threat posed by Osama bin Laden.

15. The subject was the situation in Afghanistan.

together with the Policy Unit, jointly drafted the first global overview watch-list paper for agreement by the EU's politico-military structure. By the summer of 2002, this global overview document had become the agreed basis for the Situation Centre-led joint assessment programme, and other key players, such as representatives of the Commission's External Affairs Directorate-General, had come aboard this process. A sufficient 'critical mass' of intelligence experts from some of the key civilian intelligence agencies had by then arrived in the Joint Situation Centre for it to be able to issue its first SECRET-level intelligence report.[16] Also by then, sufficient secure voice equipment had been acquired to enable a classified military intelligence report to be passed personally to Solana while he was in the field. The joint assessment process was also sufficiently underway for the first joint risk assessment to have been issued to assist in the politico-strategic level planning of the first EU-led operation. Thus, by the end of 2002, both stakeholders and customers had developed sufficient trust in the designed intelligence system and sufficient confidence in the professionalism of its output to rely on it for decision-making, which could have life or death implications for deployed personnel of the EU Member States.

As a final step in the design of the system for defence intelligence cooperation, a military intelligence structures concept paper was issued to document what had been designed. After the anticipated lengthy debates among member states' representatives,[17] it was eventually agreed by the EU Military Committee in February 2003.

16. The topic was terrorist-related.

17. Lengthy debates were anticipated because it is a challenge, with such a sensitive topic, to strike the right balance of length and level of detail in an official paper so as to generate unanimity. Writing too much may lead to the level of technical detail becoming too great for the non-technical Brussels-based representatives and to the technical experts back in the capitals starting to 'over-contribute' on detailed issues. Writing too little may lead to everyone wanting more! As far as the author is aware, no one has yet attempted to draft an official paper for agreement by the member states under the existing system of non-defence-related intelligence cooperation.

Prior to Operation Zeus, for example, the fictitious West African country had featured for some time on the EU's global overview watch list, resulting in heightened levels of input from the member states, both by their defence intelligence organisations to INT in the Military Staff and by civil intelligence services to their officers in the Joint Situation Centre. During the past two months, each meeting of the EU Military Committee and of the Political and Security Committee had received, from the Joint Situation Centre, a joint civil-military audio-visual update on the latest developments and on the assessment of future events. Hot intelligence reports had regularly been passed by Joint Situation Centre duty personnel to the High Representative prior to key top-level meetings. A key input into the overarching EU strategic concept for the mythical country, drafted by a small crisis-response coordinating team, including officials from the Commission, had been the joint risk assessment worked up in the Joint Situation Centre. The Political and Security Committee had agreed both the risk assessment and the strategic concept, having agreed the military advice received from the Military Committee, prior to deciding to recommend to Council (i.e. ministers) that Operation Zeus be launched. Officials in the Commission participated in all key elements of the decision-making process.

SOME THOUGHTS FOR THE FUTURE

One emerging challenge will be that posed by the developing EU vision of CFSP, as embodied in the new EU Security Strategy entitled *A Secure Europe in a Better World*, in particular the section on 'Policy implications for Europe'. Some commentators are still calling for a common EU threat-assessment as a pre-condition to implementing the Strategy – as already indicated, such assessments started falling into place from the summer of 2002 onwards. A key element of the Security Strategy will undoubtedly continue to be bound up in wider EU-US issues. So far as EU-led operations are concerned, the US may well continue to view them as non-threatening and often even helpful to its interests. In this context, it may well

prove possible to develop further intelligence cooperation between the EU and US intelligence and security agencies.

For example, in the mythical Operation Zeus, the US Administration signalled to the EU at a very early stage in the process of formulating the UN Security Council Resolution that, although it saw no role for NATO in such an operation, it would be prepared to offer some strategic-level capabilities bilaterally with the EU, short of committing US forces in the theatre of operations. The offer was gratefully accepted and, in addition to several C-17 sorties (strategic airlifts), the US Administration also agreed to release for EU use some suitably sanitised but still highly classified near real-time IMINT and SIGINT feeds to Operation Zeus' chain of command (i.e. to the multinationalised EU Operation HQ at PJHQ Northwood and to the multinationalised EU Force HQ deployed afloat with the carrier group).

A related challenge for intelligence cooperation in the EU will be the future of CFSP/ESDP in the context of the draft Constitutional Treaty. As far as Petersberg tasks are concerned, the draft Treaty currently proposes new wording: 'missions outside the Union for peacekeeping, conflict prevention and strengthening international security in accordance with the principles of the United Nations Charter' (Article 40); 'shall include joint disarmament operations, humanitarian and rescue tasks, military advice and assistance tasks, conflict prevention and peace-keeping tasks, tasks of combat forces in crisis management, including peacemaking and post-conflict stabilisation'. All these tasks may contribute to the fight against terrorism, including by supporting third countries in combating terrorism in their territories' (Article III-210). A 'solidarity clause' (Articles 42 and III-231), to deal – inside the Union – with the consequences of 'a terrorist attack or natural or man-made disaster', is also proposed, as is the creation of a 'European Armament, Research and Military Capabilities Agency' (Articles 40 and III-212). The High Representative's assessment, at the time of writing, is that these elements of the draft Treaty should not prove controversial. Intelligence cooperation within the EU will undoubtedly need to be broadened to embrace a whole range of new

security issues in a more coordinated manner, for example between the CFSP/ESDP and Justice and Home Affairs, so as to achieve a better interface between the external and internal counter-terrorist domains.

One challenge which the EU is already facing after May 2004 is how the CFSP/ESDP dossiers can be worked effectively with 25 members. In the field of intelligence cooperation, there will be a need to bring the intelligence elements of the new member states, many of whom may start by seeing the EU through largely NATO eyes, successfully into the EU family. All the new members will have the potential to make a valuable intelligence contribution, and all will undergo the usual security certification procedure to ensure that they have and are applying the controls needed to be able to safeguard classified EU information. Enlargement for INT itself has been based on well-argued, specific additional needs and the capabilities being offered, as opposed to any form of revised quota system. By having a 'points of contact system' with the candidate countries up and running effectively since 2001, the EU Military Staff has in effect been a market leader within the Council's General Secretariat since the start of this run-up period.

The EU has the unique capacity for an international institution of being able to add real value in a crisis-management situation, anywhere in the world, by bringing to bear a comprehensive set of tools, ranging from the political and diplomatic, through the economic and judicial, to security and defence, and backed by a developing intelligence tool. The levers of power for the different tools lie in different parts of the Union structure, principally the Council, the Commission, and increasingly, the European Parliament. The main challenge in delivering real added value in practice is therefore likely to lie in improving the lateral bridging between the EU Council and the Commission's worker teams, while seeking a more comfortable accommodation with the Parliament. In the meantime, it will be important to keep the intelligence elements of the CFSP/ESDP team mentally and physically close together. The collocation achieved to date under the Kortenberg project was a success in this respect, and should be extended if and when the opportunity is taken to move the team closer to its customer base.

Last but not least, as in any commercial enterprise, the customer's legitimate intelligence requirements must remain king. The prime purpose of the 'intelligencer' should be, while acting always within the law and within the relevant guidance, to get a high-quality product to the right people within such a timeframe that it is of real value to the customer's key activities. An intelligence management system needs to be put into effect to support each and every commander of an EU-led operation to make the best use of the intelligence capabilities made available by the states contributing to that operation. Indeed, this concept of supporting the operation commander should remain uppermost in the minds of all the national intelligence agencies when the civil or military personnel of EU member states are deployed on operations and lives are put at risk.