

This article was downloaded by: [37.218.245.204]

On: 20 November 2013, At: 08:08

Publisher: Routledge

Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



## Perspectives on European Politics and Society

Publication details, including instructions for authors and subscription information:

<http://www.tandfonline.com/loi/rpep20>

### A European Transgovernmental Intelligence Network and the Role of IntCen

Mai'a K. Davis Cross<sup>a</sup>

<sup>a</sup> ARENA Centre for European Studies, University of Oslo, Norway

Published online: 27 Sep 2013.

To cite this article: Mai'a K. Davis Cross (2013) A European Transgovernmental Intelligence Network and the Role of IntCen, Perspectives on European Politics and Society, 14:3, 388-402, DOI: [10.1080/15705854.2013.817805](https://doi.org/10.1080/15705854.2013.817805)

To link to this article: <http://dx.doi.org/10.1080/15705854.2013.817805>

PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden. Terms & Conditions of access and use can be found at <http://www.tandfonline.com/page/terms-and-conditions>

# A European Transgovernmental Intelligence Network and the Role of IntCen

MAI'A K. DAVIS CROSS

*ARENA Centre for European Studies, University of Oslo, Norway*

**ABSTRACT** *This article makes the case that the most important developments in the European intelligence arena actually have little to do with member states' willingness to cooperate. Rather, the context for the intelligence profession has changed fundamentally in the past few years in light of globalization and the information revolution, and this has made the creation of a single EU intelligence space far more likely, even despite member states' resistance. The author argues that the emerging European intelligence space is increasingly consolidating around a transgovernmental network of intelligence professionals that draw upon open-source knowledge acquisition, with IntCen at its centre. One implication of this is that the field of EU intelligence may be a rare example in which integration can be achieved before cooperation, rather than the latter serving as a stepping-stone to the former.*

**KEY WORDS:** Cooperation, EU intelligence, IntCen, integration, transgovernmentalism

## Introduction

Given the progress the European Union (EU) has made in achieving more security cooperation, and even integration (Mitsilegas et al., 2003; Smith, 2004; Jones, 2007; Spence, 2007; Mérand, 2008; Kaunert, 2011; Cross, 2011), it is appropriate to ask whether this progress also extends to the field of intelligence, a notoriously guarded area of national sovereignty and security. To what extent is there a common intelligence space in the EU today, and why? The literature on EU intelligence focuses mainly on the normative (trust) or functional (efficiency) incentives member states need to push them toward intelligence cooperation on a particular issue (Müller-Wille, 2004; Walsh, 2006; Edwards & Meyer, 2008). Recent empirical research seeks to establish that there is still a low level of political will among member states to cooperate, and a lack of desire to make use of the formal institutions set up to facilitate this. Member states tend to resist sharing intelligence with each other unless they are able to overcome the trust issues that go along with relinquishing sensitive data, and the inherent risks related to this, like putting human sources at risk. In looking at member-state motivations, most scholars have concluded that the current state of EU intelligence cooperation is quite dismal, with little hope of improving.

---

*Correspondence Address:* Mai'a K. Davis Cross Senior Researcher, ARENA Centre for European Studies, University of Oslo, Blindern N-0318, Oslo, Norway. Email: [maia.cross@arena.uio.no](mailto:maia.cross@arena.uio.no)

I argue that an exclusive focus on member states misses the mark. There is an important shift underway in the European intelligence arena that is resulting in the creation of a trans-governmental intelligence network, which includes professionals from national intelligence services, as well as from formal and informal EU institutions. Transgovernmental cooperation is defined by Robert Keohane and Joseph Nye (1974) as the process by which sub-units of governments engage in direct and autonomous interaction separate from nation states. Anne-Marie Slaughter (2004) argues that transgovernmental networks across the globe are increasingly coming together in this way to share best practices and knowhow. Government professionals like judges, legislators, and regulators seek to foster these networks so that they can do their jobs better. I argue that this dynamic is now visible in the European sphere of intelligence, and is leading to the emergence of a European intelligence space.

The timing of this process of network building can be explained through recent advances in open-source intelligence, known in the industry as OSINT. Open-source information accounts for 80–90% of all intelligence in Western governments, and it is likely growing in proportion to human and clandestine intelligence as a result of the information revolution (Rettman, January 2011). Such collaboration across national boundaries is unexpected because of the stronghold governments have on their own intelligence resources. But given that OSINT does not rely on member states political will to share information, there are strong indications that *European* intelligence is and can be derived independently from national governments (Pallaris, 2009). As an intervening variable, I argue that structural changes brought about by the Lisbon Treaty have also created fertile ground for this process of transgovernmentalism, and have placed the Joint Situation Centre (SitCen), in April 2012 re-named the EU Intelligence Analysis Center (IntCen), at the center of the European intelligence field.

In addition to IntCen, national intelligence services, Europol, the EU Military Staff (EUMS), and the European Satellite Centre are all formal groups responsible for different aspects of intelligence sharing activities within the EU. The Berne Group, Budapest Club, and Eurosint Forum are examples of key informal groups. The actors within these formal and informal groups comprise the transgovernmental intelligence network that I describe. I focus specifically on the role of IntCen as it has the mandate to deal with the most difficult and sensitive aspects of intelligence. Thus, it is a hard test for intelligence cooperation, and it is also arguably the most important contributor to the European intelligence field as it bridges both internal and external security concerns.

SitCen, the precursor to IntCen, was established in 2002 as a body that ‘monitors and assesses events and situations worldwide on a 24-hour basis with a focus on potential crisis regions, terrorism and WMD proliferation’ (Hansard, 2005). While Europol deals exclusively with crime within the EU’s borders and the EUMS is concerned with intelligence that supports Common Security and Defence Policy (CSDP) operations, IntCen’s mandate spans both and then some. It is the only actor that deals with the EU’s priority areas of defense, counter-terrorism, and crisis management at the same time. Thus, it is the fulcrum that determines whether the EU takes a comprehensive approach to achieving a common intelligence space or not. Moreover, if IntCen is at the core of an emerging trans-governmental network of European intelligence experts, it is important to take note of what this means for European security more generally.

The article proceeds as follows. First, I review the literature pertaining to intelligence cooperation, and situate my own argument in it. Second, I provide an overview of what

(little) we know about IntCen, an agency that is unusually secretive and difficult to penetrate. Third, I explain why there is an emerging transgovernmental network in which IntCen plays a crucial role. Finally, I offer some conclusions on the future prognosis for IntCen and European intelligence sharing.

### **Intelligence Cooperation**

There is a robust literature on intelligence more generally, but relatively little on EU intelligence specifically. Since EU intelligence is handled by several different groupings, both formal and informal, the limited amount of research that has been conducted on this issue is spread out, focusing on different institutions and agencies. As a result, only a small handful of scholars and think-tank experts have focused on SitCen specifically. And this is likely the first scholarly article to grapple with IntCen. Even as far as intelligence goes, IntCen is very secretive and closed off from public scrutiny, making it exceedingly difficult even to pinpoint basic elements of its structure, responsibilities, and evolving role. The few studies that examined the earlier SitCen tended to focus on the same central struggle that EU integration in general has faced: will member states be willing to give up national sovereignty to benefit from a common, European approach which combines resources and promotes efficiency?

As an important aspect of national sovereignty and security, intelligence would seem to be an area in which member states would really put up strong resistance. The fundamental dilemma that the literature addresses is that member states intuitively have a strong interest in sharing intelligence given their similar security concerns, but they are unwilling to give up sovereignty in such a secretive and sensitive area. It is acknowledged that the internally borderless nature of the Schengen area, as well as a growing Common Foreign and Security Policy, means that European security efforts will fall far short without a comprehensive approach to intelligence that includes all member states. As Björn Müller-Wille writes, 'sharing knowledge is a first step towards harmonizing views, formulating and implementing common policies, and exploiting potential synergies in the fight against new threats' (2004, p. 13). The EU already strives to integrate in combating illegal immigration, terrorism, cybercrime, organized crime, and human trafficking, among other things. A common source of intelligence analysis provides the necessary background for conducting these policies as effectively as possible.

Despite this clear need, member states are still reluctant to share intelligence. Müller-Wille outlines five main reasons for this: (1) distrust of what others will do with the intelligence, (2) concern that more EU intelligence sharing jeopardizes bilateral intelligence sharing with the US, (3) risk of free-riding, (4) loss of privileged or superior influence, and (5) fear that the intelligence will be manipulated for different ends. Geoffrey Edwards and Christoph Meyer echo the arguments about trust and free-riding, focusing in particular on the difference between those member states that are more intelligence-oriented and those that are less. They write:

... the gap in trust coupled with the risk for sources and free-riding between the national 'haves' and 'have-nots' in intelligence terms prevents a quicker evolution, institutionalization and task expansion of bodies such as SitCen. (Edwards & Meyer, 2008, p. 14)

Eveline Hertzberger's interviews of intelligence experts confirm that there is a gap between those member states like the UK, Spain, and Germany that have a lot of experience in the intelligence sector, and newer member states like Poland and Slovenia, that are relatively inexperienced (2007, p. 73).

James Walsh elaborates upon lack of trust as the central impediment to intelligence sharing among member states (2006). He argues that intelligence and trust intersect in a number of ways. First, any shared data must be protected to the satisfaction of all parties involved. Second, there must be trust that the information will not be used in a way detrimental to the interests of any of the actors. Third, intra-EU intelligence sharing must not be perceived as a threat to external forms of bilateral or multilateral intelligence sharing. His study concludes that existing EU institutions provide the technical mechanisms for sharing information, but do little to foster trust.

In a later work, Müller-Wille focuses more on the utility-driven nature of intelligence sharing, and finds weaknesses in the institutional apparatus that the EU has set up in this regard. He breaks down intelligence into a number of distinct categories, and finds that only certain areas of intelligence actually benefit from European cooperation, and this is where we are more likely to find intelligence sharing. In terms of institutional design, he argues that Europol is fundamentally flawed because 'national intelligence services constitute the primary providers of data and intelligence at the same time as they are the main customers' (2008, p. 60). Thus, it is difficult for Europol to add value. Since Europol does not have the mandate to conduct intelligence outside of the EU's borders, it is restricted to analyzing and assessing trends on a general level. Müller-Wille finds that the structure of SitCen, by contrast, is more conducive to adding value since its customers are EU decision-makers, rather than national governments.

Overall, there is a consensus in the literature that intelligence cooperation in the EU is particularly weak, and that EU institutions play only a minor role. One area where intelligence sharing is less problematic for member states is in dealing with external issues that all agree upon. Member states provide information only if there is a direct interest or benefit in doing so. For example, in areas of operational information pertaining to Common Security and Defence Policy (CSDP) operations, they are far more willing to cooperate since their own soldiers' protection in the field depends on this (Hertzberger, 2007, p. 69). EU intelligence institutions seem to have an easier time adding value on the analysis side of the equation, as opposed to the collection side.

These scholars are correct to point out that member states' national governments are resistant to sharing intelligence, but I argue that this is not actually necessary for the creation of a European intelligence space. Analyses of member-state motivations and behavior when it comes to the Europeanization of intelligence tend to neglect the most interesting developments in the field: the relationship building and networking among intelligence professionals. Increasingly, they share best practices and knowhow so that they can improve their professional skills given the new challenges brought about through globalization and the information revolution. In turn, their transgovernmental network has begun to craft a European intelligence space, even despite member states' resistance to sharing substantive intelligence.

There are many kinds of transnational actors or networks – often comprised of professionals – that scholars have identified and researched in depth. These include epistemic communities (Adler, 1987; Haas, 1992; Radaelli, 1999; Verdun, 1999; Zito, 2001; Cross, 2007, 2011), communities of practice (Adler & Pouliot, 2011), business networks,

advocacy networks (Keck & Sikkink, 1998), interpretive communities (Johnstone, 2005), and argumentative communities (Collins, 1998), among others. Many of these groups are held together by shared values and a common motivation to achieve specific goals in the international arena, whether to improve environmental regulation, protect human rights, or promote EU integration in new policy areas. Transgovernmental networks are distinctive in that they are focused less on end goals and more on processes of governance. They do not necessarily need to pursue a shared policy goal. Rather, they form a network because they share the desire to do their work better as governance professionals, and in the process they learn to trust each other. Transgovernmental networks are more informal than coalitions or committees, but do not necessarily have a specific agenda in mind (Grevi, 2008; Thurner & Binder, 2009). How does the transgovernmental network of intelligence professionals work in practice in Europe and what role does IntCen play in it?

### **What (Little) We Know About IntCen<sup>1</sup>**

Given that public information about IntCen is extremely limited – even its organizational chart is classified – it is helpful to first review what is known about this elusive organization, and its role in cultivating European intelligence. EU member states have been sharing intelligence – defined as ‘information that is tailored to assist a certain receiver’s decision-making’ (Müller-Wille, 2008, p. 52) – since at least the 1970s, but in a more ad hoc or bilateral way (Walsh, 2006). It was during the late 1990s in the wake of the Bosnian War that this process became more institutionalized. Also, 9/11 and the terrorist attacks in Madrid and London served as major impetuses towards increased intelligence sharing and the creation of SitCen (Todd, 2009). The agency, which does not have any formal legal status, was originally modeled after NATO in that member states would have the mechanism to voluntarily gather information in a central place (Wendling, 2010, p. 77). From 1998 until SitCen’s inception in February 2002, member states found themselves in the position of having agreed to the European Security and Defense Policy (now the Common Security and Defence Policy), but having no structure in place to share necessary intelligence pertaining to future missions and operations.

#### *IntCen’s Structure*

IntCen, based in Brussels, has a staff of around 80,<sup>2</sup> which includes analysts of both civilian and military backgrounds, as well as other support staff. The analysts are typically seconded from national intelligence services, and are double-hatted to both (Hertzberger, 2007, p. 69). In the wake of the Lisbon Treaty, there had been some discussion about increasing the number of analysts within IntCen (Council, 2011). In September 2010, IntCen circulated three job ads to EU institutions and member states’ foreign ministries, with a call for a deployable officer to travel to crisis areas to gather information, an open-source intelligence analyst, and a security information officer who is an expert on Asia. Presumably, this call increased the proportion of analysts on staff, effective January 2011.

The first head of IntCen was former British Diplomat William Shapcott who played a crucial role in shaping its development. The new head of IntCen is the former head of Finnish intelligence, Ilka Salmi, who Catherine Ashton appointed to the post after a competitive round of applications. This is a high-paying (€15,000/month) and prestigious

position, which requires that the individual occupying it has the trust of chief intelligence officials in the member states while still prioritizing the interests of the EU.

IntCen is comprised of decision-making bodies and implementation bodies. The decision-making bodies consist of the Intelligence Steering Board, chaired by the High Representative and Vice-President of the Commission, and the Intelligence Working Group, chaired by the directors of IntCen and the EU Military Staff's Intelligence division. The implementation bodies consist of IntCen itself, and the intelligence directorate of the EU military staff. Unlike Europol, IntCen prepares intelligence analyses for EU decision-makers, rather than authorities in the member states. Its 'customers' include High Representative Cathy Ashton, Counter-Terrorism Coordinator Gilles de Kerchove, Coreper II, PSC, the Working Party on Terrorism, the Article 36 Committee, the Policy Unit, and decision-makers in the area of police and judicial cooperation (Müller-Wille, 2008, p. 59). IntCen operates 24 hours a day and seven days a week to ensure that it is able to provide rapid updates, especially to the High Representative. It works closely with the EU Military Staff, External Action Service, and to some extent, the European Defence Agency, but not Europol, which is focused on gathering intelligence that will enable the capture and prosecution of criminals.

Between 17 and 20 EU member states, provide national intelligence to IntCen. Thus, not all member states participate, but all 27 receive IntCen's reports and analyses through their ambassadors in the Political and Security Committee. Each member state can also stipulate who is allowed to see the information, beyond those who regularly consume IntCen reports, under the so-called 'originator principle' (Rettman, November 2010). For example, they can specify that EU parliamentarians with high-level security clearance are not allowed to see the intelligence reports. Typically, when a member state wants to volunteer information to IntCen, it will convey it through its representative in IntCen. There is a secure communication system inside of the Council that can be used for this purpose (Hertzberger, 2007, p. 69). In her study, Hertzberger finds that personal contacts among these double-hatted analysts in IntCen enable better intelligence cooperation over time, and an emerging institutional culture.

### *IntCen's Mandate*

IntCen has no formal mandate to engage in intelligence *gathering*, traditionally understood, and relies to some extent on intelligence provided by member states on a voluntary basis. For example, it receives information from the French, German, and Italian spy satellites for imagery, as well as from member states' diplomatic reports. To the extent that IntCen does originate intelligence itself, this comes from open-source information, or on-the-ground observations in crises. For example, it can use US commercial satellite imagery, Internet chat-room intelligence, and media reports. In addition, IntCen analysts routinely travel to crisis zones and CSDP operation locations to gain a better sense of real conditions. They also accompany the high representative on her diplomatic trips. Finally, IntCen receives information from the EU's External Action Service delegations around the world.

IntCen's chief mandate is to provide intelligence analysis and strategic assessments to EU decision-makers, especially in the area of counter-terrorism. Each year, IntCen produces some 100 intelligence reports, 40% of which deal with terrorism assessments (Hertzberger, 2007, p. 66). In terms of rapid response, IntCen routinely provides 'flash reports' on international crises as they develop, and may also issue early warnings. IntCen constantly

monitors potential terrorist threats, the proliferation of weapons of mass destruction, and conflict-prone locations around the globe so that it is prepared to respond immediately in the event of a crisis. On a medium-term basis, IntCen provides several services involving CSDP, such as recommended procedures for crisis management, risk and situation assessments, and crisis response facilities. If analysts are on-location they may serve as the operational contact for the high representative. On a longer-term basis, IntCen focuses on strategic assessments that can build stronger resistance to terrorist attacks over time. For example, analysts deal with aviation security, cyber-security, and problems of radicalization and recruitment (Hertzberger, 2007, p. 68). Their priority is to gain a better understanding of the internal dynamics, financing, ideology, and potential targets of terrorist networks (Duke, 2006, p. 607).

More generally, it is clear that IntCen's mandate bridges both internal and external security as well as military and non-military action. This distinguishes IntCen as an EU security agency, and ensures that it is well-positioned to help EU decision-makers achieve their main security goals. The EU's comprehensive approach to security, which emphasizes the need to use both civilian and military tools, as well as the European Security Strategy, which removes the artificial divide between internal and external security, both show the necessity of an intelligence agency like IntCen. Originally, IntCen only examined external threats, but since January 2005, as a reaction to the Madrid terrorist attack in March 2004, it began to receive information from Europol about internal security issues as well (Keohane, 2008, p. 129 ; Hertzberger, 2007, p. 66). Indeed, it is now increasingly difficult to separate internal and external as well as military and non-military intelligence more generally.

In terms of internal intelligence, IntCen has had a tangible policy impact in the area of counter-terrorism and prevention of radicalization and recruitment. The division of labor between intelligence and policy-making means that the Working Party on Terrorism uses IntCen's intelligence analyses to develop action plans and policy recommendations, such as the Strategy on Radicalization and Recruitment. As a direct result of IntCen's intelligence reports, the Working Party on Terrorism encouraged member states and EU institutions to focus in particular on preventing the development of extremism in prisons, cooperating with each other to identify and prosecute jihadists in their communities, utilizing the Schengen and Visa Information Systems more fully, and protecting critical infrastructure. IntCen has been providing regular reports on individual aspects of terrorism to the Council Working Party on Terrorism since April 2005 (Council Document, 2007). Between 2005 and 2007, this Working Party adopted 75 recommendations as a result of this information (*ibid.*, p. 2).

In terms of external intelligence, IntCen has influenced crisis management operations, and has increased the EU's ability to respond quickly, like in the case of the earthquake in Haiti described below. This kind of readily accessible intelligence at the EU level is a crucial component of the EU's ability to speak with one voice in terms of common foreign policy.

Of course, IntCen is still a work in progress. The exact structure and role of IntCen under the new post-Lisbon Treaty arrangement is still evolving, as are other innovations brought about by the new treaty. For example, IntCen could conceivably move more into the area of providing policy recommendations rather than just analysis, but this still has to be decided (Rettman, February 2010). It is clear, however, that there is an increasing need for a strong, centralized crisis center that can rapidly provide intelligence in the wake of an international



emergency. Still, political will for formal intelligence sharing stemming from the member states is quite lacking when it comes to actual implementation. Nonetheless, I argue that IntCen's role is evolving as a central player in an emerging transgovernmental intelligence network.

### **A Transgovernmental Intelligence Network**

Robert Keohane, Joseph Nye, and Thomas Friedman, to name a few, characterize twenty-first century globalization as an era in which networks are getting thicker, transnational interactions are getting faster, and linkages between individuals are dramatically increasing global interdependence (Keohane & Nye, 2010; Friedman, 1999). Many security threats today are more pressing as a result of the information revolution and transnationalism, especially terrorism, organized crime, and cyber-crime. It is thus not surprising that 80–90% of intelligence comes from open sources. This means that the achievement of closer cooperation in this sensitive area no longer depends on member states' willingness to overcome sovereignty concerns and trust issues. The growing need to sort through and analyze open-source intelligence has led to the rapid development and sharing of best practices among intelligence professionals in Europe. This de-prioritizes the importance of national leaders in authorizing the sharing of intelligence. Rather, experts in IntCen, and others, are not forced to rely on information that member states choose to provide. They also have more control over how they do their work because they have the distinctive expertise to make use of OSINT.

I will build this argument in three parts: (1) how OSINT gets around trust issues on the part of member states, (2) how the increasing value of OSINT has led to the development of transgovernmental networking and sharing of best practices, and (3) how the Lisbon Treaty has served to strengthen IntCen and place it at the heart of this emerging European intelligence space.

#### *Open-source Intelligence*

The culture of mistrust among member states is becoming less of an obstacle to IntCen's work. Increasingly, the most pertinent intelligence is gathered through open-source material, such as the media, Internet chat rooms and blogs, as well as commercial satellite images, governmental reports, and deep Internet sites (those not readily accessible through standard search engines) (Rettman, January 2011). This is a recent and significant transformation in the way the intelligence profession works.

The intelligence profession has always involved a combination of both open and secret sources. But in the past few years, the technology and information revolution has meant that the balance between open and secret sources is now heavily tilted towards the former. The Council of the European Union defines open sources as:

... all the information available publicly, but not exclusively, on the Internet, which by virtue of its special importance for the maintenance of public security and for criminal investigation, should be captured, processed, evaluated, analysed and circulated to the agencies in charge of preventing and fighting crime. (Council Document, April 2010)

Open sources have many obvious advantages over clandestine sources. The latter often involves breaking the law at home or abroad, and the tricky issue of protecting human sources. When such clandestine intelligence is shared with other governments, the problems are compounded. Moreover, since the sources and methods must be kept secret, it is difficult if not impossible to check the veracity of the information. Thus, a great deal of trust is required when two or more states share intelligence transnationally (Walsh, 2006, p. 629). What if one member state has an incentive to make up information, exaggerate the accuracy of information, or share only certain parts of the information? What if the state receiving the information has an incentive to pass it on to a third state, or even mistakenly shares the information with outsiders? What if the state receiving the information has lower standards of data protection (*ibid.*, pp. 629–630)?

For these reasons, open-source intelligence can often be less complicated and more trustworthy. It is possible to replicate information searches directly, and limit the areas in which traditional, clandestine intelligence techniques are necessary. Open-source intelligence is also easier to share because it does not risk protected, human sources in third countries.

To be sure, open-source intelligence has always formed an important component of the intelligence profession, but with faster and thicker globalization patterns, this particular technique has become far more useful in the past few years. The Internet has come to encompass more countries and languages, there has been an exponential explosion in new websites that feature useful knowledge, and non-traditional threats that rely on the Internet have mushroomed (Steele, 2007, p. 132). These trends are all possible because of the nature of twenty-first century globalization.

The Internet is particularly important as an intelligence resource, but a high level of expertise is also required to draw out the most important and reliable information. As Robert Steele writes:

The Internet facilitates commerce, provides entertainment and supports ever increasing amounts of human interaction. To exclude the information flow carried by the Internet is to exclude the greatest emerging data source available. While the Internet is a source of much knowledge, all information gleaned from it must be assessed for its source, bias, and reliability. (Steele, 2007, p. 130)

Computer programs have been developed to assist with the compilation and sorting of data. The result is that intelligence analysts can increasingly draw upon computer and media skills, rather than operating as spies on-the-ground in third countries. Many EU member states engage in open-source intelligence gathering on a large scale, and still may not be willing to share their analyses with IntCen. But it is far more likely that they would share this kind of data over that obtained from clandestine sources in foreign countries given that open-source intelligence involves fewer issues of trust. The difference when it comes to open-source analyses, however, is that IntCen can engage in this type of intelligence research itself directly, thereby generating a distinctive, *European* intelligence.

#### *Networking and Best Practices*

The rising importance and use of open-source intelligence has led to increasing numbers of intelligence professionals participating in informal networks that enhance the context in

which SitCen operates. European intelligence experts are increasingly meeting in informal settings, and are re-shaping the nature of their profession in light of the information revolution and the need to engage in OSINT. Some prime examples include the Berne Group, Budapest Club, and Eurosint Forum.

The long-standing Berne Group, established in 1971 with six member states, is the body under which the heads of all 27 member states intelligence agencies and the US meet together. It focuses on operational cooperation, which EU institutions or agencies do not do (Müller-Wille, 2008, p. 55). More recently, the Berne Group established the Counter Terrorist Group in 2001, which includes the EU's 27 national intelligence services, plus those of Norway and Switzerland. Europol and SitCen have agreements in place to communicate and exchange information with the Counter Terrorist Group, connecting the formal and informal avenues for intelligence sharing. The Police Working Group on Terrorism, founded in 1979, is similar in that it operates outside of EU structures, but runs in parallel to them.

The Budapest Club, established in 2007 by an initiative of the European Commission and Hungarian government, has since its inception routinely brought together government intelligence officials and private sector experts to share ideas and techniques on collecting open-source intelligence (Rettman, 18 January 2011). The Club has even set up a secure website for participants to continue fostering their network and share counter-terrorism strategies transnationally.

Eurosint Forum, founded in 2006, is a non-governmental, non-profit organization based in Brussels that holds around five workshops a year and comprises a network of around 400 intelligence professionals, at all ranks, from member states' intelligence agencies, private-sector organizations, and EU institutions such as the EU Military Staff, SitCen, and Europol. The organization receives funding from the Commission as well as from the private sector. Each workshop usually consists of around 35 participants, but Eurosint also holds one or two larger conferences each year with more than 100 participants. According to Eurosint General Manager, Axel Dyèvre, these workshops and conferences have many opportunities for informal interactions that clearly create an atmosphere of trust, emphasize an exchange of ideas, and allow for brainstorming (personal interview, 27 June 2011, Brussels). Rather than discussing topical, and potentially confidential issues, the focus is on getting to know each other, finding areas of potential collaboration, and discussing practices. Several shared projects have emerged from these Eurosint gatherings (*ibid.*).

Eurosint also has a technology-sharing platform, called *Virtuoso*, which enables members to develop and share software that facilitates open-source research. The development of *Virtuoso* is funded by the EU Commission, but is not technically an official project of the EU. The main purpose of it is to develop a standardized platform, which will enable the intelligence professionals who use it to have their own separate systems, but to integrate the overarching structure to facilitate sharing (*ibid.*). Dyèvre said that this common framework helps to break down the walls in the European intelligence space because dealing with best practices is not as sensitive as dealing with actual intelligence. Nonetheless, once there is a certain comfort with discussions on the more technical level, this may facilitate exchange on a substantive level.

Given that the seminars and workshops hosted by the Budapest Club and Eurosint Forum are informal in nature and encourage the development of personal friendships and contacts, they provide an ideal environment for building relationships. Participants

are aware that the culture of European intelligence is changing, and it is moving towards fulfilling the spirit of the Lisbon Treaty (Rettman, 18 January 2011). Because both of these groups focus on open-source intelligence and the development of suitable technology, it is easier for participants to share best practices without jeopardizing state secrets. This has likely resulted in a shared body of professional norms and substantive norms about how best to develop government policy related to intelligence. In 2007, Sandro Calvani, Director of the United Nations Interregional Crime and Justice Research Institute, wrote, 'personal contacts and informal arrangements play a crucial role in the initiation and maintenance of intelligence cooperation relations' (2007).

### *The Impact of the Lisbon Treaty*

It is clear that the transgovernmental network of intelligence professionals is both horizontal (across member states) and vertical (between the national and European levels), but there is much to suggest that IntCen will play an increasingly important role in the European intelligence community. This is largely because of the impact of the Lisbon Treaty. Before Lisbon, IntCen was embedded in the Council Secretariat. Now, IntCen is subsumed within the European External Action Service (EEAS). The EU Military Staff, including its Watch Keeping Capability, was also transferred to the EEAS on 1 January 2011 (Council Document, December 2010). This may seem like a simple bureaucratic reorganization, but it is not. These relocations have likely enhanced the efficiency and effectiveness of IntCen. The hierarchy, chain of command, and organization are much more streamlined. The EU is establishing specific guidelines for the EEAS's intelligence support, and the emphasis is on higher quality intelligence provided much more rapidly than in the past (interview with Gunter Eisl, Director of Intelligence in the EUMS, 27 June 2011).

At a broad level, the Lisbon Treaty itself reflects the exigencies of a globalizing world as it pertains to new areas of security and defense. Lisbon got rid of the pillar system set up under the Maastricht Treaty, which separated internal security (third pillar) from external security (second pillar), and from the Community area of decision-making (first pillar). The pillar system had become seriously outdated some time ago given that most of the third pillar had rapidly migrated into the first, especially in the years following 9/11. The line between internal and external security quickly blurred as well. Cross-pillarization was the natural tendency practically from the beginning.

At a closer level, the relocation of IntCen from the Council Secretariat to the EEAS has a major bearing on its power to engage in intelligence gathering, in addition to analysis. Previously, IntCen could not task the EU's 136 Commission delegations around the world with gathering vital information on its behalf. Now, it can (House of Lords, 2004). Previously, IntCen had to make an additional effort to bridge its work to internal security matters through Europol and the Commission, but these were always awkward relationships. Now, with the whole field of foreign policy merged into a single hierarchy under High Representative Ashton, IntCen's role becomes far more coherent. As a result, it is far more likely to be useful, especially in crisis scenarios that require a quick response.

The 12 January 2010 Haiti earthquakes provides a good example of how IntCen now operates in practice in dealing with real time crises (EUISS, 2010). Naturally, IntCen staff monitor international events on a non-stop basis, so the officer on duty at the time immediately became aware of the earthquake (at 11pm Central European Time), and notified the IntCen Crisis Response Manager who was on standby. The Crisis Response

Manager determined that the earthquake would likely require a political response from the EU, and he alerted High Representative Ashton around midnight. The first humanitarian aid and civil protection (ECHO) experts were in Haiti 14 hours after the earthquake. Meanwhile, IntCen began an intensified process of open-source intelligence gathering. Because the earthquake had damaged communications infrastructure, it became apparent that IntCen was hampered in its efforts to find out what was happening on the ground. Moreover, the EU delegation based in Haiti was not able to function as a provider of information. The head of delegation had been evacuated for injuries, the Chargé d'Affaires died in the disaster, many other staff members were hurt, and the delegation building was crumbling.

Ashton dispatched two IntCen officers who arrived in Haiti on 18 January, and set up a temporary EU office in the logistical base of the UN Stabilization Mission in Haiti. Ashton tasked them with gathering information, assisting with consular issues, evacuating EU citizens, and setting up communications between Haiti and Brussels. The IntCen officers were able to establish a satellite antenna and begin real time communication with Brussels. They also coordinated with the other EU actors in the area, as well as the UN. Given IntCen's flow of information, Ashton was able to lead discussions on potential civil and military actions that the EU could take to help alleviate the disaster. On 25 January, the Foreign Affairs Council agreed to Ashton's proposal to set up EUCO Haiti, a crisis coordination cell that would enhance the operations that IntCen had begun to set up. Overall, especially given that the earthquake occurred during the gap between when the Lisbon Treaty entered into force and when Lisbon institutions were established, IntCen's contribution was successful.

Ashton has herself envisioned a much more rapid response time for IntCen compared to the pre-Lisbon period, with the intelligence unit directly under her command. If a crisis breaks out, she now has direct authority to send IntCen analysts on-location to report back to her. In the past, a discussion in the Political and Security Committee on whether or not to engage IntCen was required. The role of open-source intelligence gathering was crucial, and demonstrates the far more central role of IntCen in the broader European intelligence network.

### **Conclusions and Implications**

I have argued that there are numerous contextual developments that have important causal significance in the world of EU intelligence, beyond the usual arguments about member-state preferences. Much of this stems from the process of globalization, which has acquired a different speed and quality in the twenty-first century. The technology revolution and information explosion have turned open-source intelligence into the dominant method of information collection in the intelligence field. This method is particular well suited to discovering non-traditional security threats that rely on the Internet for communication, and to detecting the first signs of humanitarian crises or revolutions, as in the Middle East. The EU's current security priorities are cyber-crime and terrorism, which gives IntCen the opportunity for real value added, beyond what individual member states can produce on their own. In the wake of the Lisbon Treaty, the EU now has a new intelligence chief, and an opportunity to expand its functions and capabilities. In its new home within the EEAS, IntCen has a streamlined command structure in support of a single foreign policy hierarchy. Ashton has the power to send analysts immediately out to crisis locations to collect on-the-ground information shortly after the start of a crisis.

The globalization context is particularly conducive to the strengthening of an intelligence transgovernmental network that can actively shape a European intelligence space. Network members create both vertical and horizontal ties, and informal meetings enable intelligence analysts to share best practices and develop shared norms of communication. This type of interaction is likely leading to the construction of a robust, single European open-source intelligence project. I would suggest that IntCen already reflects a high degree of intelligence integration, even if there is still a low degree of cooperation among member states directly. Moreover, as IntCen consolidates its new role, it becomes a better partner for intelligence communities in third countries, especially that of the United States. Since 9/11, the transatlantic intelligence community has grown, and a stronger SitCen enables further areas of cooperation in achieving US-EU shared security goals.

As a final word, it is important to consider the connection between intelligence and democratic transparency. As I have already alluded to, IntCen is highly secretive and low profile. It is the only agency that has no website, and it is very difficult for the public and researchers to gain access to staff members. The head of IntCen rarely even appears in public (Hertzberger, 2007, p. 68). IntCen is unusually secretive, even in comparison to national intelligence agencies. Since IntCen is *not* the equivalent of a European Intelligence Agency, the EU and member states have felt justified in shielding it from public scrutiny and accountability.

There is an informal parliamentary group that has access to some of IntCen's documents, but because of the originator principle, the group is easily prevented from engaging in scrutiny. They are also prevented from discussing any of the intelligence they receive outside of their narrow group. The main reason for these restrictions is that member states do not support a stronger relationship between IntCen and the European Parliament. They are very concerned about what happens with the intelligence that they relinquish to IntCen. For their part, IntCen analysts believe that if they keep a low profile, they might gain more trust from member states.

IntCen's extremely closed nature does deserve some criticism, and it already receives quite a bit. For example, a 2009 story in *The Telegraph* criticized as 'Orwellian' the Commission-funded computer programs that enable SitCen analysts to compile Internet data, including personal information (Johnstone, 2009). The main concern is that IntCen has a lot of EU funding and resources at its disposal and yet it is an impenetrable agency that few understand. IntCen's role has been expanding since at least 2005 when it began to work on internal security issues. Now that it has been given a more central role within the EEAS it is imperative that the agency allow some cracks in its secretive façade. It need not go so far as to jeopardize European security interests, but since it is able to rely so heavily on open-source intelligence, it need not bend over backwards to show the member states that it can keep a low profile. The simple reality is that member states are only able to provide a small fraction of the intelligence that IntCen can acquire itself.

## Notes

<sup>1</sup> Any research on intelligence encounters hurdles because the product of intelligence officers must remain confidential. Since IntCen officials do not grant interviews or release documents, there is very little information available on how it operates on a day-to-day basis.

<sup>2</sup> It was reduced from a staff of around 110–120 when it was still Sitcen (Rettman, February 2010), and had a somewhat broader remit, such as the Crisis Room for keeping track of media reports, and services involving consular support, among others. Intcen is more focused specifically on gathering and analyzing intelligence; some of the more secondary functions that existed under Sitcen, are no longer part of Intcen.

## References

- Adler, E. (1987) *The Power of Ideology: The quest for technological autonomy in Argentina and Brazil* (Berkeley, CA: University of California Press).
- Adler, E. & Pouliot, V. (2011) International practices, *International Theory*, 3(1), pp. 1–36.
- Calvani, S. (2007) Foreword, in: E. Hertzberger, *Counter-terrorism Intelligence Cooperation in the EU*, Turin: UNICRI, p. 1.
- Collins, R. (1998) *The Sociology of Philosophies: A global theory of intellectual change* (Cambridge, MA: Harvard University Press).
- Council of the EU Document 17444/10. 6 December 2010, Brussels.
- Council of the EU Document 5626/11, 24 January 2011, Brussels. Still classified.
- Council of the EU Document 9037/10, 27 April 2010, Brussels.
- Council of the EU Document 7261/07 EXT 1, 12 March 2007, Brussels.
- Cross, M. K. D. (2007) *The European Diplomatic Corps: Diplomats and international cooperation from Westphalia to Maastricht* (Basingstoke: Palgrave)
- Cross, M. K. D. (2011) *Security Integration in Europe: How knowledge-based networks are transforming the European Union* (Ann Arbor: University of Michigan Press)
- CSDP Newsletter, Issue 10, Summer 2010.
- Duke, S. (2006) Intelligence, security, and information flows in CFSP, *Intelligence and National Security*, 21(4), pp. 604–630.
- Edwards, G. & Meyer, C. (2008) Introduction: Charting a contested transformation, *Journal of Common Market Studies*, 46(1), pp. 1–25.
- EU Institute for Security Studies (2010) Crisis response to the Haiti earthquake – an EU SITCEN perspective, *CSDP Newsletter*, Issue 10, Summer.
- Friedman, T. (1999) *The Lexus and the Olive Tree* (New York: Anchor Books).
- Grevi, G. (2008) Transgovernmental cooperation under CFSP: Institutional and normative profiles, in: M. Dony & L. S. Rossi (Eds) *Démocratie, cohérence, et transparence: principes constitutionnelles de l'Union européenne?* (Brussels: University of Brussels).
- Haas, P. (1992) Introduction: Epistemic communities and international policy coordination, *International Organization*, 46(1), pp. 1–35.
- Hansard, House of Commons, 27 June 2005.
- Hertzberger, E. (2007) Counter-terrorism intelligence cooperation in the EU, *European Foreign and Security Studies Policy Program UNICRI*.
- House of Lords (2004) Examination of witnesses: William Shapcott, 3 November, London.
- Johnstone, I. (2005) The power of interpretive communities, in: M. Barnett & R. Duvall (Eds) *Power in Global Governance*, pp. 185–204 (Cambridge: Cambridge University Press).
- Johnstone, I. (2009) EU funding 'Orwellian' artificial intelligence plan to monitor public for 'abnormal behavior', *The Telegraph*, 19 September. Available at: <http://www.telegraph.co.uk/news/uknews/6210255/EU-funding-Orwellian-artificial-intelligence-plan-to-monitor-public-for-abnormal-behaviour.html> (Accessed on 16 July 2013).
- Jones, S. (2007) *The Rise of European Security Cooperation* (Cambridge: Cambridge University Press).
- Kaunert, C. (2011) *European Internal Security: Towards supranational governance in the area of freedom, security and justice* (Manchester: Manchester University Press).
- Keck, M. & Sikkink, K. (1998) *Activists Beyond Borders: Advocacy networks in international politics* (Ithaca, NY: Cornell University Press).
- Keohane, D. (2008) The absent friend: EU foreign policy and counter-terrorism, *Journal of Common Market Studies*, 46(1), pp. 125–146.
- Keohane, R. O. & Nye, J. S. (1974) Transgovernmental relations and international organizations, *World Politics*, 27(1), pp. 39–62.
- Keohane, R. & Nye, J. S. (2000) Globalization: What's new? What's not? (And so what?), *Foreign Policy*, 118, pp. 104–119.

- Mérand, F. (2008) *European Defence Policy: Beyond the nation state* (Oxford University Press).
- Mitsilegas, V., Monar, J. & Rees, W. (2003) *The European Union and Internal Security: Guardian of the people? (One Europe or several?)* (Basingstoke: Palgrave).
- Müller-Wille, B. (2004) For our eyes only: Shaping an intelligence community within the EU, *Occasional Paper 50*, Paris, European Union Institute for Security Studies.
- Müller-Wille, B. (2007) The effect of international terrorism on EU intelligence cooperation, *Journal of Common Market Studies* 46(1), pp. 49–73.
- Müller-Wille, B. (2008) The effect of international terrorism on EU intelligence cooperation, *Journal of Common Market Studies*, 46(1), pp. 49–73.
- Pallaris, C. (2009) OSINT as Knowledge, Activity and Organization: Trends, Challenges and Recommendations, Swiss Federal Institute of Technology Zurich, pp. 1–16.
- Radaelli, C., (1999) The public policy of the European Union: Whither politics of expertise?, *Journal of European Public Policy*, 6(1), pp. 757–774.
- Rettman, A. (2010) Ashton picks Finn to be EU ‘spymaster’, *EUObserver.com*, 17 December.
- Rettman, A. (2010) EU diplomats to benefit from new intelligence hub, *EUObserver.com*, 22 February.
- Rettman, A. (2010) Secret documents group was like ‘bad Le Carre novel’, MEP says, *EUObserver.com*, 18 November.
- Rettman, A. (2010) EU diplomats to benefit from new intelligence hub, *EUObserver.com*, 22 February.
- Rettman, A. (2011) EU intelligence services opening up to collaboration, *EUObserver.com*, 18 January.
- Smith, M. E. (2004) *Europe’s Foreign and Security Policy: The institutionalization of cooperation* (Cambridge: Cambridge University Press).
- Slaughter, A. (2004) *A New World Order* (Princeton, NJ: Princeton University Press).
- Spence, D. (Ed.) (2007) *The European Union and Terrorism* (London: Harper).
- Steele, R. (2007) Open source intelligence, in: L. Johnson (Ed.) *Handbook of Intelligence Studies*, pp. 129–147 (New York: Routledge).
- Turner, P. W. & Binder, M. (2009) European Union transgovernmental networks: The emergence of a new political space beyond the nation state?, *European Journal of Political Research*, 48(1), pp. 80–106.
- Todd, M. (2009) Could Europe do better on pooling intelligence?, *Security & Defence Agenda Round Table Report*, October 26, Brussels.
- Verdun, A. (1999) The role of the Delors Committee in the creation of EMU: An epistemic community?, *Journal of European Public Policy*, 6(2), pp. 308–328.
- Walsh, J. (2006) Intelligence-sharing in the European Union: Institutions are not enough, *Journal of Common Market Studies*, 44(3), pp. 625–643.
- Wendling, C. (2010) Explaining the emergence of different European Union crisis and emergency management structures, *Journal of Contingencies and Crisis Management*, 18(2), pp. 74–82.
- Zito, A. (2001) Epistemic communities, collective entrepreneurship and European integration, *Journal of European Public Policy*, 8(4), pp. 585–603.