Epistemic policy networks in the European Union's CBRN risk mitigation policy

Abstract: This paper offers insights into an innovative and currently flagship approach of the European Union (EU) to the mitigation of chemical, biological, radiological and nuclear (CBRN) risks. Building on its long-time experience in the CBRN field, the EU has incorporated methods familiar to the students of international security governance: it is establishing regional networks of experts and expertise. CBRN Centres of Excellence, as they are officially called, aim to contribute to the security and safety culture in different parts of Africa, the Middle East, South East Asia and South East Europe, in the broadly-construed CBRN area. These regional networks represent a modern form of security cooperation, which can be conceptualized as an epistemic policy networks approach. It offers flexibility to the participating states, which have different incentives to get involved. At the same, however, the paper identifies potential limitations and challenges of epistemic policy networks in this form.

Keywords: security governance; epistemic policy network; European security; CBRN; foreign policy

Introduction

The European Union (EU), including the Council of Ministers but also the European Commission, has a long history of developing preventive policies in the field of chemical, biological, radiological and nuclear (CBRN) weapons, materials and know-how. Already at the beginning of the 1990s, the European Community initiated technical assistance - known as the Technical Aid to the Commonwealth of Independent States (TACIS) - with the security and safety of nuclear installations constituting an important component of this assistance. The low profile of the Community's activities channelled through TACIS allowed the European Commission to develop its assistance relatively uncontested, apart from the criticism directed at the actual effectiveness of TACIS (Sodupe and Benito, 1998). As the Cold War years were becoming increasingly distant, and in the wake of Russia's new-found assertiveness of 2000s, the priorities of the EU have started to shift.

In parallel to the policies developed in the Council of Ministers, the European Commission has decided to shift its CBRN risk reduction policies to other regions – it went global. The experience of TACIS remained important as a learning experience. When, in 2009, the European Commission first outlined the rationale for CBRN Centres of Excellence (CoE), it was building on its experience of managing TACIS: ‘Taking into account the lessons learned through the TACIS programme and the first IfS IP [Instrument for Stability, Indicative Programme], the IP 2009-2011 intends to move away from an “ad hoc”, centralized approach to promoting coherent, integrated regional networks’ (European Commission, 2009, p. 7). The CBRN risk mitigation regional networks, in the form of EU CBRN CoE, constitute the empirical focus of this paper. CBRN CoE are the networks of experts, facilities and training in regions considered by the EU to be vulnerable in terms of criminal acts (proliferation, organized crime and terrorism), natural disasters (pandemics) and accidents (industrial catastrophes).

The participation in such networks is voluntary and countries involved are not obligated to do anything – they merely request support to develop necessary capacities addressing a specific set of CBRN-related risks. The CBRN CoE is an innovative project launched by the EU in 2009, with the purpose of ‘developing comprehensive tailored training and assistance packages’ in the field of CBRN risk mitigation (European Commission, 2009, p. 8). It is implemented jointly with the United Nations Interregional Crime and Justice Research Institute (UNICRI). These training and assistance packages are directed at the regions currently including different parts of Africa, the Middle East, South East Asia and South East Europe. The networks are still in the early stage of their development, but permanent Regional Secretariats have already been established in Amman, Algiers, Tbilisi, Manila and Rabat. The Regional Secretariats act as focal points for coordinating national and regional project development and for establishing long-term, transnational networks of CBRN experts. The initiative is financed through the EU’s Instrument for Stability.

The empirical developments in the EU’s international security governance raise the question about the best practice in mitigating contemporary security challenges and risks, and how it relates to existing scholarship. Admittedly, the scholarship on International Relations has been rather slow in moving beyond the inter-state paradigm and accounting for some of the recent empirical developments. The concept of security community, while taking into consideration ideational factors, offers a rather static and territorially-bound image of security cooperation. Consequently, together with the idea of risk community, it is contrasted with a more promising concept of security governance. Security governance, while also limited in important ways, offers a much more accurate account of the empirical developments such as the CBRN CoE project. The paper is structured in a way which demonstrates this point. Following the brief discussion of contemporary security and risk environment, the case study of CBRN CoE is introduced and conceptualized as an example of epistemic policy networks. Subsequently, the paper revisits the scholarship on contemporary security cooperation in order to evaluate in what ways it falls short of accounting for the case study at hand. Security governance is most promising in this respect, due to the central role of policy networks typically associated with this form of cooperation.

Security and risk

Globalization is constantly changing the nature of security threats and risks facing modern societies. While more traditional security threats have not disappeared, we are increasingly confronted by man-made and natural uncertainties, threatening the lives and well-being of vulnerable societies. Karen Lund Petersen (2012) has offered an excellent overview of different ways in which the studies of security and risk speak to each other in recent scholarship. It is not the intention to repeat her arguments. Instead, it is important to zoom in on one element of the security-risk debate, asking how the concept of risk sometimes displaces the concept of security, and what implications this process has for policy-making. For Beck, the scale of modern-day risks, from environmental disasters to terrorism and conflict, reflects the triumph of modernity. The society is increasingly vulnerable to risks not *in spite of*, but as *a side effect of* modernization. This fact challenges the basic logic of Weberian means-end rationality, because ‘all attempts at rational control give rise to new “irrational”, incalculable, unpredictable consequences’ (Beck, 2009, p. 18-19). Table 1 summarizes the key differences between threats, with their inherent logic of means-end rational action, and risks, which stem from the very nature of modern rationality.

Table 1

The Cold War rivalry is often presented in the literature as an example symbolising the distinction between threat and risk. In short, the threat of the Soviet Union was quantifiable, present, finite, with recognized intentions and possible to eliminate. In contrast, the risk of the CBRN proliferation from the former Soviet Union countries is unquantifiable, transcends time and space and is infinite. Moreover, the intentions of potential proliferators are unknown and the risk requires on-going risk-mitigation measures. In his welcome speech during the Brussels-based conference ‘Towards a Global Network of Crisis Rooms’ in 2013, Graham Hutchings from Oxford Analytica clearly articulated the nature of modern risks:

> Crises and catastrophes do not respect frontiers. They do not respect spatial frontiers, temporal frontiers. They are not respecters of culture and context, of wealth, status and gender. They are genuinely international. We have got used in the last few decades to a global manufacturing industry, a global financial industry, global tourism and the like. What I submit we have not yet got used to is a global industry or practice of crisis detection, of crisis analysis, crisis monitoring and, most importantly, crisis response (Hutchings, 2013).

Indeed, the methodology for addressing modern risks and transnational security problems remains work in progress. For Beck, transnational cooperation is the key. States must admit that, as autonomous units, they are powerless vis-à-vis modern risks and that the only solution is the pooling of sovereignty (Beck, 2009, p. 41). In this context, the aforementioned initiative of the EU, aiming to mitigate CBRN-related risks through the establishment and facilitating of policy networks, is innovative. The primary purpose of CBRN Centres of Excellence is to (a) move the EU's CBRN assistance beyond the territories of the former Soviet Union; and (b) develope an innovative approach to CBRN risk governance, drawing on its experience in the countries of the former Soviet Union, primarily Russia (European Commission, 2009, p. 7; Kaunert and Zwolski, 2013). In fact, the officials involved in CBRN CoE argue that 'if successful, it may be the first time that the EU develops a comprehensive approach to threat and risk reduction beyond Russia' (Dupré and Servais, 2012, p. 2). If pooling of sovereignty is a necessary condition for preventing and addressing modern risks, expertise-centred policy networks appears as a suitable method for facilitating inter- and trans-national cooperation.

The EU and prevention through epistemic policy networks

For the purpose of the argument, epistemic policy networks are defined as *formal, expertise-centred structures, purposefully-created by international actors, to address a specific set of security risks over the short-to-long term, through capacity-building activities*. This definition may be more restrictive than it is generally the case in the scholarship on policy network theory (Enroth, 2011). It only includes policy networks which have been intentionally created to serve a particular policy purpose. In other words, policy networks in this definition serve as the instruments with a formal mandate and a delineated scope of activities. Essentially, however, this definition is similar to the understanding of policy networks proposed by Rhodes (1996). The primary difference may stem from the notion of network self-organization in Rhodes' definition, which means that they are autonomous and self-governing. However, while epistemic policy networks, as defined here, are created and managed by formal international actors, some degree of autonomy and self-governing is inevitable. Further, Rhodes also emphasizes that governance is about *managing* networks: 'As British government *creates* agencies, bypasses local government, uses special purpose bodies to deliver services, and encourages public-private partnerships, so networks become increasingly prominent among British governing structures' (1996: 658).

Regardless of the definitional nuances, policy networks in general face similar challenges. On the side of achieving effectiveness, these challenges include the problem of coordination and trust-building. Coordination, as Mark Bevir (2009: 56-57) notes, 'occurs when two or more policy actors pursue a common outcome and work together to produce it'. Minimum coordination is the precondition of interdependence, thus the success of networks depends on the degree of coordination among the members. This variable, in turn, is heavily influenced by trust (Enroth, 2011). Unfortunately, the methodology of building trust is elusive. Rathbun (2012) offers a design for understanding the role of trust in international cooperation by juxtaposing rationalist, constructivist and social psychological models. In rational institutionalism, states naturally distrust each other. In order to facilitate trust, which can be called strategic trust, states create institutions. In social constructivism, trust follows shared identity and culture. In this model, we have to analyse how intra-regional relations are constructed based on the history of amity versus enmity, particularly in the security sphere. In social psychological arguments, to trust is a disposition independent of any situational circumstances. States that are 'general trusters', are more likely to cooperate than states that are 'general non-trusters', unless they have evidence that they should not trust in a particular case. In this model, we should look for indicators of how 'generally trusting' particular states are, based on domestic politics, including the ideology of the government in power.

Epistemic policy networks as formal structures created by international (state and non-state) actors do not have to be confined to policy areas involving the mitigation of risks or security threats. At the same time, however, if global uncertainties and different security threats become increasingly diffused and transnational, policy networks involving experts are increasingly considered by international actors as appropriate means of addressing problems. International organizations, in particular, are keen to adopt this arguably innovative methodology. In their approach to modern security governance, international organizations intend to adopt long-term outlook, promote transnational networks of experts, emphasize the voluntary character of cooperation and encourage local ownership. In this project-based approach, actors in vulnerable regions are invited to jointly apply for required resources (expertise, funding), to address a specific set of risks and security threats. As a consequence, international organizations hope to transform mistrust into confidence and national focus into regional cooperation.

Can this approach be effective? Epistemic policy networks entail addressing a specific set of security risks over (a) short-to-long term; and (b) through capacity-building activities. This property of the networks is embedded in the discussion concerning compliance in international relations, launched by Chayes and Chayes (1993). In this debate, scholars argue over the best strategies (management or enforcement) to make states behave in accordance with international norms and rules. Arguably, managerialist strategies are most popular in areas where scientific and technical expertise is crucial (von Stein, 2013). In the context of the EU, the consensus seems to have emerged that the European Commission employs the mixture of both strategies to ensure compliance of its member states with EU rules (Börzel, 2003; Tallberg, 2002). While such a mixed approach may be suitable in the EU's internal compliance strategies, external security policy through epistemic policy networks is based on managerial strategies, involving 'non-confrontational, forward-looking and facilitative' (Raustiala and Slaughter, 2002, p. 543) approaches. In this context, the EU develops and facilitates epistemic policy networks based on the assumption that non-compliance with international security norms and rules is often inadvertent and stems from resource constraints rather than malicious intentions. In response to these constraints, networks aim to assist participating parties with resources relevant to tackle a given set of security risks within a short and (mainly) longer term. Having established the working definition of epistemic policy networks, the reminder of this paper applies it to the case study of the EU's CBRN CoE.

Epistemic policy networks as a formal structure

In the last few years, the CBRN CoE initiative has emerged as the flagship EU approach to CBRN risk mitigation, which is the result of two factors. Firstly, the CBRN non-proliferation was allocated with the largest proportion of the Instrument for Stability budget under article 4, defining the EU's assistance in the stable conditions for co-operation (€266 million for the years 2007-13 = 13 per cent of the total budget) (European Commission, 2007). Secondly, in the pool available for CBRN non-proliferation, the CBRN CoE initiative is defined as the ‘number one’ priority area for the EU (European Commission, 2009; 2012). This is unsurprising, considering that the EU has long planned to move its assistance beyond the former Soviet Union and the CBRN CoE enabled the EU to go global. Further, in light of the criticism directed towards its previous assistance programmes (Sodupe and Benito, 1998), the EU planned to change the methodology of its assistance, by decentralising it and focusing on ‘local ownership’. Moreover, CBRN CoE reflect the priorities of the United Nations Security Council Resolution 1540, which provides the international context for the EU’s initiative. The following section demonstrates how the EU has adopted epistemic policy networks as an approach to mitigate CBRN-related risks. The discussion is organized around three attributes of epistemic policy networks: their formality, their expertise-centrism, and their capacity-building activities.

The CBRN CoE project is developed within the framework of the Instrument for Stability - one of the external assistance financial instruments of the EU, intending to bridge the gap between security and development aims in EU external policy (Zwolski, 2012a; b). Translating the rationality of the Instrument for Stability into the institutional realities of the EU, the instrument can be considered the first attempt to ‘define the Grey Zone between the Council’s CFSP, ESDP and the Commission’s development policy, a step that might complete existing programmes and encourage active conflict prevention’ (Beer, 2006, p. 34). The Instrument for Stability is divided into two parts, regulated by articles 3 and 4. The article 3 enables the EU to act in situations of urgency, crisis or emerging crisis. Around three quarters of the instrument’s budget (total of €2.062 billion for 2007-2013) is allocated for this purpose. The CBRN CoE, on the other hand, is an article 4 project. The article 4 regulates the assistance that can be deployed in stable conditions for co-operation. The main priority area for this component of the Instrument for Stability includes ‘risk mitigation and preparedness relating to chemical, biological, radiological and nuclear materials or agents’ (European Parliament and the Council, 2006). Following the Lisbon Treaty reforms, the CBRN CoE are coordinated by the European Commission (Joint Research Centre, Development and Cooperation-EuropeAid) and the European External Action Service (EEAS), with the potentially greater role of the member states (Dupré and Servais, 2012). UNICRI is involved in the implementation.

Epistemic policy networks are expertise-centred

Nowhere is the need for expertise as apparent as in the field of CBRN security, involving a myriad of technical and political challenges. CBRN CoE, as a form of transnational security governance, aims to fill the need for expertise at national and regional levels. Among the key objectives of the initiative are (a) to provide CBRN training to participating countries; (b) to support participating countries in developing legal, administrative, and technical measures; and (c) to provide a coherent package of training and assistance covering CBRN matters such as export control, illicit trafficking, crisis response and redirection of scientists (European Commission, 2009). In order to accommodate this need for expertise, CBRN CoE are implemented through the system of Regional Secretariats, which to date have been established in Amman, Algiers, Tbilisi, Manila and Rabat. They operate as regional focal points to coordinate the implementation of CBRN-related projects and to bring together relevant regional expertise and resources.

> The regional secretariat of the Centre of Excellence established in each region is the driving force of the initiative. It coordinates administrative support provided by the EU contractor and local personnel, and the expert support from the EU, partner countries or international organizations. It also interfaces with the authorities of the hosting country, and finally with the EU delegation and EU member states embassies in the host country (Bril, 2013: 239).

At the national level, the CBRN CoE are developed and implemented through the co-operation of the so-called National Focal Points of the Partner Countries, which are countries outside the EU participating in the networks. They develop regional CBRN risk mitigation projects through the Regional Secretariats (Mignone, 2013). The National Focal Points of the Partner Countries can comprise a variety of actors as diverse as first responders, police, customs, CBRN agencies, ministries, academia and intelligence (Winfield, 2011, p. 50). They form teams of around 20-30 experts, representing a country at the regional level through co-operation with Regional Secretariats. Such teams may play important integrative roles, because ‘in many cases it is the first time that many of the representatives that cover the whole of CBRN in a country have sat down and talked to each other’ (Winfield, 2011, p. 50). At the same time, however, the highly specialized expertise required puts a strain on the availability of human resources in the EU and in participating countries (Mignone, 2013, p. 7). Furthermore, with 29 projects implemented by 18 entities in 42 different countries, as was the case in mid-2013 (Schmidt, 2013, p. 1), there is a risk that the expertise which is available will not be optimally utilized (Mignone, 2013, p. 7).

A wide range of expertise required can indeed put a strain on the availability of human resources for the optimal implementation of CBRN CoE. The European Commission's Joint Research Centre, together with UNICRI, partially provides the necessary expertise, but it is also the role of Regional Secretariats to pool regional resources, for example through the organization of round table meetings of National Focal Points. In parallel to the CBRN CoE initiative, the EU has recently established 'a nongovernmental non-proliferation network, bringing together foreign policy institutions and research centres' – the EU Non-proliferation Consortium (Council, 2008, p. 10). The goals of the network, in addition to stimulating dialogue, were specified as follows: (a) to advise Council officials on non-proliferation matters; (b) to advance the EU's role in non-proliferation, notably by advising the representative of the EU's High Representative for Foreign Affairs and Security Policy; and (c) to raise awareness in third countries about the need to work multilaterally and in cooperation with the EU on CBRN-related issues. In relation to CBRN CoE, the Consortium should be able to assist the EU as well as national teams in the partner countries in identifying relevant sources of expertise.

Epistemic policy networks support capacity-building

The CBRN CoE embed the managerial approach to security risk governance, which is reflected in their exclusive focus on capacity-building activities over the short-to-long term. The networks offer carrots without the threat of sticks – an approach which bears inevitable limitations. CBRN CoE are intended to offer a novel methodology to compliance through capacity building, based on a number of principles, including: (a) networking, partnerships, optimising existing capabilities; (b) addressing specific needs through projects; (c) strengthening regional safety culture through pooling local resources and expertise. Michael Thornton, the project coordinator, confirms that CBRN CoE operate based on managerial assumptions, in which non-compliance results from insufficient resources, rather than adversity:

> In all the countries that we have been to so far, and we have been to quite a few, they have all indicated that they would like to get something out of this, and because it is voluntary they can pick and choose. One country could say that they have no legislation in terms of biosafety or biosecurity, and can we help them with that? Ok, we can help with that. Another one could say that they have a significant problem with illicit nuclear trafficking, so therefore they want to

> strengthen export control and border monitoring. It is individual, there is no one size fits all (Winfield, 2011, p. 48).

In practice, the scope of the projects funded by the EU through the framework of CBRN CoE is broad. For example, one of the latest projects approved for implementation concerns improving CBRN emergency response in Iraq, Jordan and Lebanon through ‘inter-agency, locally trusted structure for the coordination, establishment and implementation of CBRN incident response throughout the region’ (CBRN CoE Newsletter, 2013: 2). Many projects concern the development of best practice in preventing CBRN accidental and human-made disasters. One of them is implemented by the German Office of Economics and Export Control (BAFA) in 15 countries across 4 regions, including African Atlantic Façade, Central Asia, Middle East and North Africa. This project is intended to last 24 months, which is a typical length of CBRN CoE projects. Its main objectives are to (a) develop procedures and guidelines to deter illegal trans-boundary shipments of CBRN materials; (b) build trust among different entities, agencies, public institutions and other stakeholders; (c) develop a sustainable knowledge sharing system; and (d) improve regional inter-agency cooperation (www.cbrn-coe.eu). The EU, through BAFA, intends to consult partner countries individually, but also to organize a system of seminars – one central and subsequently in each region.

There are a number of factors affecting the outcomes of CBRN CoE, however. These include the commitment of EU member states; access to relevant expertise; interaction by different project teams; the ability to establish geographical and thematic priorities; establishing an accurate verification mechanism and communicating the outcomes to a wider audience (Dupré and Servais, 2012; Mignone, 2013). Other challenges are associated with the fact that the cooperation with partner countries is voluntary, it involves important matters of security risks, and the countries are asked to think through the lenses of regional needs, and not merely national interests.

This approach is fundamentally different from the traditional role of international organizations facilitating interstate co-operation. It requires national leaders in the Middle East, North Africa, South East Europe, South East Asia and African Atlantic Façade to adjust their thinking about preventing CBRN risks. Leaders in these regions are implicitly asked by the EU and UNICRI to operate under the assumption that their interests in CBRN matters are not so different as to prevent them from developing joint security projects. Building local and regional trust is the intended original contribution of the EU's CBRN CoE to the environment where different nuclear research and technical centres already exist. In fact, project coordinators argue that in such a sensitive field as CBRN, trust and confidence are pivotal for improving security in a long term: 'We will not make a real difference in threat/risk reduction on the mere substance of our projects. Something has to come first: *Trust and Confidence Building Measures*' [original emphasis] (Dupré and Servais, 2012, p. 2).

Politics and power relations in epistemic policy networks

Epistemic policy networks, as a form of transnational security governance, do not eliminate politics and power relations. While international organizations may present their project-based initiatives as voluntary, de-centralized and cooperative, the underlying structures and motives require scholarly attention. The EU's own initiatives aiming to prevent security emergencies, such as the CBRN CoE, should not be considered *a priori* as any different. In fact, the coordinators of CBRN CoE envisage one of many potential problems in managing CBRN risk mitigation projects:

> Secretariats of the Centres of Excellence will be small structures composed of ten people. They will be subject to pressure by national CBRN teams wanting to put forward national agendas. Impartiality skills and corruption awareness training (financial and technology vigilance) will be offered to progressively uncouple the regional team experts from their national origin (Dupré and Servais, 2012, p. 5).

Other questions concern the actual motivation of national actors in regions as diverging as the Middle East, North Africa, South East Europe, South East Asia and African Atlantic Façade to participate in the EU's sponsored initiative and the extent of possible socialization. The EU certainly intends for its network-based methodology to transform the behaviour in regions of proliferation concern. This objective, project coordinators believe, can only be achieved by building 'trust and confidence measures' (Dupré and Servais, 2012, p. 2). At different levels, however, we can identify potential problems that international organizations may encounter when exercising managerial, project-based approach in international security governance; some of these challenges were discussed. Most importantly, the EU is challenged by the fact that security policy has traditionally been considered as deeply engrained in the competence and identity of sovereign states. At the deeper level, we may argue that 'even the most institutionalized bodies of knowledge advanced by international organizations are contested and continually criticized' (Sending and Neumann, 2011, p. 240). This contestation and criticism often stems from the heterogeneous and contradictory character of norms and values projected by international organizations (Sending and Neumann, 2011, p. 240).

Modern forms of security cooperation: (un)fit for purpose?

Thus far, the paper has discussed the nature of modern security challenges and risks. While it seems that there is universal agreement that the pooling of national sovereignty is necessary to address security threats and risks, the method of actually achieving this goal remains work in progress. In this context, the paper has introduced the case of the EU's CBRN CoE and conceptualized it as epistemic policy networks. Policy networks enable and can help to facilitate inter- and trans-national cooperation. The EU seems to have taken this principle into account when developing its own methodology, hoping to address risks comprehensively, including their legal, regulatory, enforcement and technical aspects. If this method, relying on networking, expertise-sharing and capacity-building is an example of good practice, where does it leave us vis-à-vis the scholarship on modern forms of security cooperation? Arguably, new forms of security cooperation have not replaced the more traditional ones, most notably the alliance and concert. Instead, states are often simultaneously members of different types of security multilateralism, such as NATO and the EU. At the same time, scholars have been pointing to the limitations inherent in the alliances and concerts, most importantly their predominant focus on the military aspects of security and the assumption that all states remain Westphalian in character (Sperling, 2009: 4). Modern forms of security cooperation enable, and even require, a stronger involvement of non-state actors, such as international organizations. Further, they are more appreciative of the fact that security threats are more diffused and are often more accurately conceptualized as sociological, economic or natural risks (Petersen, 2012).

Risk and security community

In response to the changing nature of modern risks, a group of scholars have developed the idea or risk community. Williams (2008), drawing on the earlier works by Christopher Cocker, conceptualizes risk community and argues that because all risk perceptions are subjective, successful risk management requires shared norms, values and institutions among the members of the community. For Williams, the West represents an example of risk community. However, in order to become more effective in mitigating problems such as CBRN proliferation, terrorism or disease, the West cannot rely on the established institutional structures. Instead, it must address such challenges through coalitions of the willing, such as the one assembled by the United States for the operation in Iraq. One does not need to dig deep, however, to identify problems with conceptualising the system of *ad hoc* international military alliances as an example of risk communities suitable to address problems in a manner similar to the methodology of CBRN CoE. Two problems arise immediately. First, coalitions of the willing are mostly inter-governmental and do not make use of the opportunities offered by transnational cooperation. When addressing modern security problems and risks, transnational cooperation is the key, as has been aptly discussed earlier in the paper. Second, risk communities, as conceptualized by Williams, are deeply unstable, largely depending on domestic politics in participating countries. This, again, runs contrary to the ideas behind epistemic policy networks, which aim to bring the elements of stability and predictability into the unpredictable and unstable world of risk and security threats.

The limitations of risk communities, as conceptualized by Williams (2008), seem to be absent from security communities, as originally developed by Karl Deutsch and associates (1957), and more recently thoroughly revised by Emanuel Adler and Michael Barnett (1998). In their original conceptualization, Deutsch *et al.* (1957) have distinguished between amalgamated and pluralistic security communities. The first type, exemplified by the United States, exists whenever there is a ‘formal merger of two or more previously independent units into a single larger unit, with some type of common government after amalgamation’ (Deutsch *et al*., 1957: 6). In contrast, pluralistic security community is characterized by ‘the legal independence of separate governments’. This definition of security community serves as a point of departure for Adler and Barnett, but they identify two limitations of the original conceptualization. First, they argue that the concept has been ill-defined and thus is difficult to operationalize. Second, it has lacked the social constructivist dimension, pointing to the role of norms, values and identity in security community.

As a result, they define security community as ‘a region of states whose people maintain dependable expectations of peaceful change’ (Adler and Barnett, 1998: 30). Focusing on the pluralistic type of security community, they further differentiate between (a) loosely-coupled security communities, in which states ‘maintain dependable expectations of peaceful change’ (1998: 30) and (b) tightly-coupled security communities, which additionally involve collective aid and a system of rule on the verge of sovereign state and transnational, post-sovereign system. In their conceptual design, Adler and Barnett (1998) also recognize three characteristics of security communities. First, in accordance with the social constructivist approach, security communities have shared identities, values and meanings. Second, the relations within a community are many-sided and direct. Third, communities involve reciprocity and some degree of altruism. Among the examples of security communities are Western Europe and the Euro-Atlantic community. The latter, as Adler (1998) argues, has been developed in a most significant way by the Organization for Security and Cooperation in Europe (OSCE), although NATO and the EU have also played important roles.

To what extent can security community account for the empirical developments involving epistemic policy networks? Admittedly, the EU’s CBRN CoE involve a system of rule on the border of sovereign statehood and transnational, post-Westphalian system. States remain important actors, particularly among the partner countries. At the same time, supranational structures, most notably the European Commission and the EEAS, are involved in managing the networks. Consequently, we should abandon the quest for clear-cut classifications in this case. The EU itself is a hybrid system, thus we should only expect that the policies it develops will have state-based, transnational and supranational elements. There is a different problem, however, when applying the lens of epistemic community to the case study at hand. It concerns the territoriality-bias in the idea of security community – the word ‘community’ precludes the existence of insiders and outsiders. Both Western Europe and the Euro-Atlantic community are defined geographically, whilst the EU’s initiative is functional – it can be (and in fact is) global in nature. It is also limited in scope. The countries involved in CBRN CoE do not have to fulfil the security community criteria to work together on CBRN-related problems. For example, initially, they don’t need to share identities, values and meanings. Instead, it is sufficient if they decide that there may be some value to them in joining the network and gradually develop mutual trust. As the networks are organized geographically, mutual trust and confidence in CBRN matters can emerge over time, but it is unlikely to emerge across all regions involved in the CBRN CoE project and involve all security matters. Consequently, security community is ill-equipped to account for the recent emergence of epistemic policy networks in the form of CBRN CoE. The paper now turns to security governance (Krahmann, 2003a; Webber *et al*. 2004; Kirchner, 2006; Kirchner and Sperling, 2007; Schroeder, 2011).

Security governance

The relationship between security community and security governance is far from straightforward. On the one hand, Sperling (2009) recognizes different types of security community *as forms of* security governance. On the other hand, Krahmann and Kirchner clearly differentiate security governance from security communities. In her conceptualization, Krahmann (2003a) acknowledges that security governance shares some qualities with Adler and Barnett's (1998) approach to Deutsche's security community. At the same time, however, she points out that security governance differs from security community because it involves a range of formal and informal institutions; it offers a better framework to capture the changing coalitions of member states as well as increasing reliance on private actors; and it accounts for security arrangements which are more fluid and flexible. Kirchner (2006) complements this list with the observation that security communities are more exclusive than security governance systems. While the existence of a security community precludes outsiders, or 'the other', the system of security governance can include varying degrees of participation – an issue discussed with reference to CBRN CoE. Furthermore, Kirchner points out that there is some tension in how the role of international institutions is perceived in the security community scholarship. Security governance, in contrast, is unambiguous in that the institutions play a central role in promoting security inside and outside of the security governance system.

There are different conceptualizations of security governance, including various attempts at summarising this strand of the scholarship (Bevir and Hall, 2013; Christou *et al.*, 2010: 342-46; Kirchner and Domínguez, 2011: 5-11; Schroeder, 2011: 30-36; Sperling, 2009: 4-6). The most common approach is to adapt the 'governance turn' in international relations (Rosenau and Czempiel, 1992), European Studies (Kohler-Koch and Rittberger, 2006) or national politics (Rhodes, 1997) to the problem of security cooperation. Some important recent contributions in this journal have undertaken an effort to take the 'security governance' scholarship to the next analytical level. Notably, Sperling and Webber (2014) argue that systemic factors have been neglected at the expense of agency in this strand of scholarship. Thus, they ask 'how and why security actors behave in the aggregate and whether that behavior reflects wider systemic properties' (2014: 1). Ehrhart, Hegemann and Kahl (2014), in the same issue, aim to deepen the analytical value of 'security governance' by transforming this concept into critical questions and enhance it as a critical tool.

Schroeder (2011: 31) neatly encapsulates the key characteristics of 'governance' as referring to 'a mode of political decision-making beyond hierarchical government of a traditional interventionist state'. This is a very broad definition, but in fact it may even be too restrictive, because governance does not have to take place only at the 'decision-making' stage. As Rosenau (1995) argues, governance may include 'systems of rule', which entail 'control' and ‘steering’. Schroeder further notes that governance ‘provides a framework for understanding the fragmentation of authority to new actors and levels, and it enables a comprehensive analysis of interactions in a sector characterized more by complex decision-making and nested responsibilities for action’ (2011: 31).

This complex decision-making in the system where authority has become more fragmented points to one important attribute of the security governance system – policy networks. Within these networks, the position of different kinds of experts has become central, not least due to the myth of ‘expert knowledge’, which is highly institutionalized by the established Western educational system (Meyer and Rowan, 1977: 344). Writing his contribution over 90 years ago, Weber (1978, p. 975) has already noted that ‘[t]he more complicated and specialized modern culture becomes, the more its external supporting apparatus demands the personally detached and strictly objective *expert*’. Weber was writing about the growing complexity of culture long before the digital age revolutionized the sources and nature of security threats and risks, introducing new levels of complexity and technological progress (Giddens, 1990; Beck, 1999). In consequence, we require experts to address these risks at least as much as states needed tanks to conduct warfare in the 20th century. Policy networks involving experts, or epistemic policy networks, constitute therefore a crucial element of the contemporary system of security governance.

As a consequence, the idea of security governance appears most appropriate to account for the recent empirical developments discussed in this paper. Most importantly, it overcomes two shortcomings of security communities. Firstly, it does not have to be limited to a particular territory – it can involve functional cooperation on particular security problems, i.e. CBRN security governance, counter-terrorism governance, etc. Secondly, it emphasizes the role and importance of non-state actors, most notably international institutions. This is unsurprising, considering the fact that, in the literature to date, security governance has been mostly applied to the EU. In this paper, the focus has not been so much on the EU itself, which could be defined as a post-Westphalian security community. Rather, the focus has been on what the EU does in international security, which can be accounted for by the concept of security governance better than by other concepts. Policy networks have traditionally been at the core of the security governance agenda, whether at the level of the EU (Krahmann, 2003b) or sub-national politics (Rhodes, 1997). In fact, the two concepts are sometimes used interchangeably. This brings us back to Beck’s recommendations for more transnational cooperation and the pooling of sovereignty. Is the network-based security governance, as exemplified by the EU's CBRN CoE, the best method for preventing and mitigating contemporary transnational risks?

While it clearly has the benefit of enabling and supporting transnational cooperation, it is not free from limitations. Schroeder (2011), for example, questions the implicit assumption that horizontal forms of cooperation have a higher problem-solving capacity than hierarchical systems. She also points to the neglect of political power and formal authority in the governance-oriented analyses. When we apply these concerns to the case study discussed in this paper, and the idea of epistemic policy networks more broadly, three main limitations become apparent. Firstly, international entities may see insufficient value in establishing knowledge-based networks by considering them as either too costly and/or ineffective. In particular, national governments may find it politically too risky to commit resources to policies which may not produce noticeable positive outcomes before the next round of elections. It does not come as a surprise that 'many current political practices in established democracies are very ill-suited to the task of delivering long term policy goals' (Stoker, 2012: 5). Secondly, even when actors recognize the value of expertise in addressing a given security challenge, different scenarios are possible which can hamper the emergence of the networks. For example, there may be the deficit of sufficient expertise and knowledge about a given security problem, such as new types of pandemic disease. More fundamentally, the legitimacy of policy networks may be challenged when there are conflicting expert views or because experts are selected, rather than elected democratically. Scholars have been pointing to these risks by coining terms such as epistocratic dominance and technocracy (Ellul, 1954; Eriksen, 2011). Thirdly, epistemic policy networks rely on the voluntary cooperation of all actors involved. International entities establishing and facilitating these networks may only try to persuade states to become members and to commit extra resources, modify behaviour, technical standards, regulations, etc. The outcome of this persuasion does not have to be positive, however, particularly in sensitive matters involving security problems.

Conclusion

Notwithstanding some of the potential and actual limitations of security governance, there currently is no better framework to account for the empirical developments in international security cooperation involving policy networks. Prevention is the key in this approach and in the case of the EU's CBRN CoE it involves mainly the transfer of best practice; providing training and mentoring; and the development of guidelines and legislation. The future research may include the comparison of the EU's CBRN CoE and other examples of epistemic policy networks, such as the initiatives developed under the auspices of (International Nuclear Security Education Network), or coordinated by (International Network for Nuclear Security Training and Support Centres), the International Atomic Energy Agency (IAEA, 2012). Of course, the so-called managerialist approaches to international compliance with (security) norms, of which epistemic policy networks are an example, are most appropriate in areas where scientific and technological expertise is crucial (von Stein, 2013). The identified limitations of the security governance will require further scrutiny. Most importantly, we need to keep asking whether horizontal forms of cooperation have a higher problem-solving capacity than hierarchical systems, ideally with reference to particular case studies. This implicit assumption has populated over two decades of governance research. While it is too early to answer this question with regards to the EU's CBRN CoE, project coordinators already signal the limits of the bottom-up approach:

> [P]rocedures are necessary for the accession of new States, to withdraw a programme, to establish consortiums including not only Member States but also, crucially, international organizations such as the IAEA, NGOs such as the ICRC, and universities. Procedures and directives are needed to establish the respective roles of the Commission, the EU diplomatic arm (EEAS), delegations, and embassies (Dupré, 2012: 1).

Undoubtedly, the CBRN CoE project offers interesting avenues for further research. Scholars interested in the evolution and performance of the EU in international security governance, including the prevention of man-made and natural emergencies, are presented with interesting new case studies. Theoretical tools and frameworks, such as the 'international practice' (Adler and Pouliot, 2011) approach, may be helpful in uncovering interesting patterns of the EU's policy internationally. Scholars focusing on the role of governmental and non-governmental transnational actors, such as epistemic policy networks, may be attracted by the scope of the EU's CBRN CoE initiative and how transnational links are being developed to strengthen cooperation. Finally, analysts studying regional/transnational/global security governance will find a growing number of international security governance initiatives relying, at least partially, on project management. The challenges and opportunities associated with capacity building of this type are worth further research.

References

Adler, E. and Barnett, M., 1998. *Security Communities*. Cambridge: Cambridge University Press.

Adler, E. and Pouliot, V., 2011. International Practices. *International Theory*, 3(1), 1–36.

Adler, E., 1998. Seeds of peaceful change: the OSCE's security community-building model. *In*: E. Adler and M. Barnett, eds. *Security Communities*. Cambridge: Cambridge University Press, 119-160.

Beck, U., 1999. *World Risk Society*. Cambridge: Polity.

Beer, A. 2006. Final Report. Conference on Greening Foreign and Security Policy: The Role of Europe', European Parliament, 6 and 7 December.

Bevir, M. and Hall, I., 2013. The Rise of Security Governance. *In*: M. Bevir, O. Daddow and I. Hall, eds. *Interpreting Global Security*. Abingdon: Routledge, 31-61.

Bevir, M., 2009. *Key Concepts in Governance*. London: Sage.

Börzel, T.A., 2003. Guarding the treaty: The compliance strategies of the European Commission. *In*: T.A. Börzel and R.A. Cichowski, eds. *The State of the European Union vol. 6: Law, Politics and Society*. Oxford: Oxford University Press, 197-220.

Bril, L-V., 2014. The European Union CBRN Regional Cenrtes of Excellence initiative. *In*: O. Maier, ed. *Technology Transfers and Non-Proliferation: Between control and cooperation*. Abingdon: Routledge, 230-43.

CBRN CoE Newsletter, 2013. *Implementation under way*, No. 7, November.

Chayes, A. and Chayes, A.H., 1993. On compliance. *International Organization,* 47(2), 175-205.

Christou, G., Croft, S., Ceccorulli, M. and Lucarelli, S., 2010. European Union Security Governance: Putting the Security back In. *European Security*, Special Issue, 19(3), 341-59.

Council, 2008. Council Conclusions and new lines for action by the European Union in combating the proliferation of weapons of mass destruction and their delivery systems, 17172/08, 17 December.

Deutsch, K. *et al*., 1957. *Political community and the North Atlantic area; international organization in the light of historical experience*. Princeton: Princeton University Press.

Dupré, B., 2012. ‘The challenges facing the European Union Centres of Excellence’, *The Non-Proliferation Monthly*, Issue 71, October.

Dupré, B. and Servais, P., 2012. The EU CBRN Risk Mitigation Centres of Excellence. *CBRN CoE Newsletter* 4, October.

Ehrhart, H-G., Hegemann, H. and Kahl, M., 2014. Towards security governance as a critical tool: a conceptual outline. European Security, DOI: 10.1080/09662839.2013.856303.

Ellul, J., 1954, *The Technological Society*. New York: Vintage Books.

Enroth, H., 2011. Policy Network Theory. *In*: M. Bevir, ed. *The SAGE Handbook of Governance*. London: SAGE, 19-35.

Eriksen, E.O., 2011. Governance between expertise and democracy: the case of European security. *Journal of European Public Policy*, 18(8), 1169-89.

European Commission, 2007. The Instrument for Stability: Strategy Paper 2007-2011.

European Commission, 2009. The Instrument for Stability - Multi-annual Indicative Programme 2009–2011, C(2009) 2641, 8 April.

European Commission, 2012. Multi-annual Indicative Programme 2012-2013 for assistance in the context of stable conditions for cooperation under the Instrument for Stability’, C(2012) 5584 final, 20 August.

European Parliament and the Council, 2006. Regulation (EC) no 1717/2006 of the European Parliament and the Council of 15 November 2006 establishing an Instrument for Stability. *OJEU* L 327.

Giddens, A., 1990. *The Consequences of Modernity*. Cambridge: Polity in association with Blackwell.

Hutchings, G. 2013. Speech during the opening of the ‘High-level Conference on Managing Complex International Crises: Towards a Global Network of Crisis Rooms’, Brussels, 3-4 December.

IAEA, 2012. Nuclear Security Report 2012. International Atomic Energy Agency, GOV/2012/41-GC(56)/15, 31 July.

Kaunert, C. and Zwolski, K., 2013. *The EU as a global security actor: a comprehensive analysis beyond CFSP and JHA*. Basingstoke: Palgrave.

Kirchner, E. and Domínguez, R., 2011. Regional Organizations and Security Governance. *In*: Kirchner, E. and Domínguez, R., eds *The Security Governance of Regional Organizations*. Abingdon: Routledge, 1–22.

Kirchner, E. and Sperling, J., 2007. *EU Security Governance*. Manchester: Manchester University Press.

Kirchner, E., 2006. The Challenge of European Union Security Governance. *JCMS: Journal of Common Market Studies*, 44(5), 947–68.

Kohler-Koch, B. and Rittberger, B., 2006. Review Article: The 'Governance Turn' in EU Studies. *JCMS: Journal of Common Market Studies*, 44(S1), 27–49.

Krahmann, E., 2003. Conceptualizing Security Governance. *Cooperation and Conflict*, 38(1), 5–26.

Krahmann, E., 2003. *Multilevel networks in European foreign policy*. Burlington: Ashgate.

Meyer, J.W. Rowan, B., 1977. Institutionalized Organizations: Formal Structure as Myth and Ceremony. *American Journal of Sociology*, 83(2), 340–63.

Mignone, A., 2013. The European Union's Chemical, Biological, Radiological and Nuclear Centres of Excellence Initiative, *Non-Proliferation Papers*, No. 28, June.

Petersen, K.L., 2012. Risk analysis - A field within security studies? *European Journal of International Relations*, 18(4), 693-717.

Rathbun, B.C., 2012. *Trust in International Cooperation*. Cambridge: Cambridge University Press.

Raustiala, K. and Slaughter, A-M., 2002. International law, international relations and compliance. *In*: W. Carlsnaes, T. Risse and B.A. Simmons, eds. *Handbook of international relations*. London: SAGE, 538-558.

Rhodes, R.A.W., 1996. The New Governance: Governing without Government, *Political Studies*, XLIV, 652-67.

Rhodes, R.A.W., 1997. *Understanding Governance*. Buckingham: Open University Press.

Rosenau, J.N. and Czempiel, E.O., eds. 1992. *Governance without Government: Order and Change in World Politics*. Cambridge: Cambridge University Press.

Rosenau, J.N., 1995. Governance in the Twenty-first Century. *Global Governance*, 1(1), 13–43.

Schmidt, K., 2013. Introduction, *CBRN CoE Newsletter*, No. 6, June.

Schroeder, U.C., 2011. *The Organization of European Security Governance: Internal and External Security in Transition*. Abingdon: Routledge.

Sending, O.J. and Neumann, I.B., 2011. Banking on power: how some practices in international organization anchor others. *In*: E. Adler and V. Pouliot, eds. *International practices*. Cambridge: Cambridge University Press, 231-54.

Sodupe, K. and Benito, E., 1998. The Evolution of the European Union's TACIS Programme, 1991-96. *Journal of Communist Studies and Transition Politics*, 14(4), 51–68.

Sperling, J. and Webber, M., 2014. *Security governance in Europe: a return to system*. European Security, DOI: 10.1080/09662839.2013.856305.

Sperling, J.A. 2009. Introduction: Security Governance in a Westphalian World. *In*: C. Wagnsson, J.A. Sperling and J. Hallenberg, eds. *European Security Governance: The European Union in a Westphalian World.* Abingdon: Routledge, 1–15.

Stoker, G., 2012. Economic recovery and the politics of the long-term. In *SPERI Inaugural Conference*, Sheffield, UK, 16-18 July 2012.

Tallberg, J., 2002. Paths to compliance: Enforcement, management, and the European Union. *International Organization*, 56(3), 609-643.

Von Stein, J., 2013. The engines of compliance. *In*: J.L. Dunoff and M.A. Pollack, ed. *Interdisciplinary perspectives on international law and international relations*. Cambridge: Cambridge University Press, 477-501.

Webber, M., et al., 2004. The Governance of European Security. *Review of International Studies*, 30(1), 3–26.

Weber, M., 1978. *Economy and Society*. Berkley: University of California.

Williams, M.J., 2008. (In)security studies, reflexive modernization and the risk society. *Cooperaiton and Conflict*, 43(1), 57-79.

Winfield, G., 2011. The Network of Excellence. *CBRNe World*, Spring, pp. 47–52.

Zwolski, K., 2011a. Unrecognised and unwelcome? The role of the EU in preventing the proliferation of CBRN weapons, materials and knowledge. *Perspectives on European Politics and Society*, 12(4), 477-492.

Zwolski, K., 2011b. The external dimension of the EU's non-proliferation policy: Overcoming inter-institutional competition. *European Foreign Affairs Review* 16(3), 325-340.

Zwolski, K., 2012a. The EU and a holistic security approach after Lisbon: Competing norms and the power of the dominant discourse. *Journal of European Public Policy*, 19(7), 988–1005.

Zwolski, K., 2012b. The EU as an international security actor after Lisbon: Finally a green light for a holistic approach? *Cooperation and Conflict*, 47(3), 68-87.

Table 1. The differences between threats and risk.

Threat	**Risk**
Can be controlled rationally	Rational control leads to new uncertainties
Quantifiable, capabilities can be counted	Unquantifiable
Occupy the present	Transcend time and space
Intentions are recognized	Intentions are unrecognized or don't exist
Threats are finite	Risks are infinite
Threats can be eliminated	Risk-management never ends